

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 passthrough 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

	cisco Web Secur	S000V ity Virtual Appliance		w	eb Security Appliance	is get
٨	Reporting	Web Security Manager	Security Se	rvices	Network	S
	Domain Map	efined.				
	Copyright © 2003-2019	Cisco Systems, Inc. All rights rese	erved. Privacy S	tatement		

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.

•	Reporting	Web Security Manager	Security Services	Network	System Administration	
	Domain Map	Add Domain				
	Domain Map					
		Domain Name:	whatsapp.com)		
		Order:	1	_		
		IP Addresses: (?	2a03:2880:f22d:c3:face:l 2a03:2880:f22d:c3:face:l 2a03:2880:f22e:c3:face:l 2a03:2880:f22e:c3:face:l 2a03:2880:f22f:c3:face:l 2a03:2880:f22f:c3:face:l 2a03:2880:f230:c3:face:l 2a03:2880:f230:c5:face:l 2a03:2880:f230:c5:face:l 2a03:2880:f230:c5:face:l	000c:0:177/128, 000c:0:167/128, 000c:0:167/128, 000c:0:177/128, 00c:0:177/128, 00c:0:167/128, 000c:0:167/128, 000c:0:167/128, 000c:0:167/128,)))))))))))))))))))))))))))))))))))))	
	Cancel			_		Submit

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.**

Reporting	Web Security Manager	Security Services	Network	System Administr	ration
Domain Map	Authentication Identification Profiles SaaS Policies				
Success — Setting Domains Add Domain	Web Policies Decryption Policies Routing Policies Access Policies Overall Bandwidth Limits		_	_	_
Order 1	Data Transfer Policies Cisco Data Security Outbound Malware Scanning External Data Loss Prevention Web Traffic Tap Policies				Delete
Copyright © 2003-2019	SOCKS Policies Custom Policy Elements Custom and External URL Catego Define TimelRanges and Quotas Domain Map Bypass Settings	ry Statement			

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

Custom and External URL Categories	
Categories List	
Add Category No custom and External URL Categories are defined.	1

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

ustom and External URL Category	
Category Name:	whatsapp
List Order:	1
Category Type:	Local Custom Category
Sites: 🕐	whatsapp,com Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order. (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)
	Regular Expressions: ?
	Enter one regular expression per line.

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

	Reporting	Web Security Manager	Security Services	Network	System Administration	
Cus	stom and I	External URL Cate	gories			
Suc	cess - The O	ustom URL Category "whatsa	app" was added			
Cate	ogories List					
Ad	id Category					
Orde	er Category		Category Type	Last Updated	Feed Content	Delete
1	whatsapp		Custom (Local)	N/A	-	8

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.

Decryption Policies

Policie	Policies							
Add F	Policy							
Order	Group	URL Filtering	Web Reputation	Default Action	Delete			
	Global Policy Identification Profile: All	Monitor: 85	Enabled	Decrypt				
Edit F	Policy Order							



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.

Decryption Policy: Add Group

Policy Settings	
✓ Enable Policy	
Policy Name: 🕐	WHAT.DEC.POL
Description:	
Insert Above Policy:	1 (Global Policy) V
Policy Expires:	Set Expiration for Policy
	On Date: MM/DD/YYYY
	At Time: 00 🔽 ; 00 🔽
Policy Member Definition	1
Membership is defined by the combination of the f	ollowing options. All criteria must be met for the policy to take effect.
Identification Profiles and Users:	All Identification Profiles 🗸
	If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTIPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.
Advanced	Define additional group membership criteria.
Cancel	Submit

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

Use the Advanced Category), or User	options to define or edit membership by proxy port, subnet, Time Range, destination (URL Agents.
The following adva	anced membership criteria have been defined:
Proxy Ports:	None Selected
Subnets:	None Selected
Time Range:	No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
URL Categories:	None Selected
User Agents:	None Serected

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

Decryption Policies: Policy "WHAT.DEC.POL": Membership by URL Categories

Advanced Membership Definition: URL Category	Y	
Select any row below to use that URL Category as n	membership criteria. Leave all rows unselected if membership by URL Cat	egory is not desired.
Custom and External URL Categories		
		Add
Category	Category Type	Select all
whatsapp	Custom (Local)	
Predefined URL Categories		

e. Click Done.

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

Decryption Policies

Succes	ss — The policy group "WHAT.DEC.POL" v	was added.			
Policie	5				
Add F	Policy				
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	WHAT.DEC.POL Identification Profile: All URL Categories: whatsapp	Monitor: 1	(global policy)	(global policy)	Ŵ
	Global Policy Identification Profile: All	Monitor: 85	Enabled	Decrypt	
Edit F	Global Policy Identification Profile: All Policy Order	Monitor: 85	Enabled	Decrypt	

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

Decryption Policies: URL Filtering: WHAT.DEC.POL

Custom and External URL Cate	gory Filtering							
These URL Categories are defined	d as group membership criter	ia. All other	categories are	not applicab	le for this p	oolicy.		
		Use	Override Global Settings					
		Global Settings	Pass Through	Monitor	Oecrypt	Drop ?	Quota-Based	Time-Based
Category	Category Type	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
😗 whatsapp	Custom (Local)	_	1				-	

h. Commit the changes.

Re	eporting	Web Security Manager	Security Services	Network	System Administration	
Decr	yption Po	olicies				
Success - Settings have been saved.						
Policies						
Add P	olicy					
Order	Group		URL Filtering	Web Reputation	Default Action	Delete
1	WHAT.DEC.P Identification R URL Categorie	DL Profile: All s: whatsapp	Pass Through: 1	(global policy)	(global policy)	8
	Global Policy Identification	Profile: All	Monitor: 85	Enabled	Decrypt	
Edit Policy Order						
ŝt P	URL Categorie Global Policy Identification P olicy Order	s: whatsapp Profile: All	Monitor: 85	Enabled	Decrypt	



Use cases:

1. WhatsApp.com

Here is the screenshot when WhatsApp is not connecting:

(it gets stuck on the loading window)

WhatsApp		-	□ ×
	To use WhatsApp on your computer:		
	1. Open WhatsApp on your phone	C	
	2. Tap Menu 🕴 or Settings 🞯 and select WhatsApp Web		
	3. Point your phone to this screen to capture the code		
	Need help to get started?	Keep me signed in	
			- 11

After configuring the Domain Map:

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

WhatsApp		N
+	0	+ …
Q Search or	start new chat	
	No chats	

2. Skype

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

Skype	- 🗆 X
\leftarrow	
Give me a call when you re back.	I
9:59 PM Call 59s	
Today 10:40 AM Missed call	
	Sending Hello
🙂 Type a message 🔂	E (†

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

Sky	pe				_		×
←	0 L	ast seen 41m ago 🖾 Gallery 🤇	२ Find			Ç	о ⁺
		Mohit, 9:40 PM					
		Give me a call when you're b	oack. 🙂				
			9.59 PM				
			Call 59s				
			– Today				
			11·27 AM				
			Call decline	d			
					Hellc	AM :	
		Type a message		ß	¢		

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 "%(" :



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.