Disable ESMTP Inspection on FTD/ASA running FTD code from FMC/CLI

When ESMTP inspection in enabled on ASA/FTD device and you try to telnet to exchange server, you see rows of Asterisks and cause failure with sending email to exchange server. As these devices are you gateway, when you try to connect your on-prem exchange with cloud-based solutions like O365 or Mimecast, you have this issue.

ESMTP is enabled by default on ASA and ASA running FTD code, whereas it is disabled by default on FTD appliances.

You can go to verification section to identify if ESMTP is enabled on your firewall.

Verification of ESMTP inspection from CLI

- 1. Connect to ASA/FTD CLI via SSH
- 2. Enter command 'system support diagnostic-cli' to enter ASA CLI
- 3. Enter command 'enable' to gain admin access, enable password is blank (just press Enter)
- 4. Enter command 'show running-configuration'
- 5. Scroll down to the end section "policy-map global_policy"
 - a. If you see '*inspect esmtp*', this means ESMTP inspection is enabled, else means it is disabled.





Disable ESMTP Inspection via FMC GUI

- 1. Login to FMC GUI
- 2. Navigate to **Object** → **FlexConfig** → **TextObject**
- 3. Open 'disableInspectProtocolList'
- 4. Add 'esmtp' to the list and Save
- 5. Navigate to **Devices** → **FlexConfig**
- 6. Create '**New Policy**' or '**Edit**' existing policy you have and is applied to the device you want to push this setting
- Select 'Default_Inspection_Protocol_Disable' from left tab and click right-arrow add button to add it to "Selected Prepend FlexConfigs"
- 8. You can click on **magnifying lens** button to see the configuration it will push and verify it has **ESMTP** in the list
- 9. Click on '**Policy Assignment**' and add the device from the list you want to deploy this configuration to device.
- 10. Save and Deploy the configuration
- 11. Once deployed, use the Verification step to verify that 'inspect esmtp' is now removed

Overview Analysis	Policies	Devices	Objects	AMP	Intelligence		
Object Management Intrus		on Rules					
Text Object Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can hav							
Standard	^	Name					
 Address Pools IPv4 Pools IPv6 Pools Application Filters AS Path Cipher Suite List Community List Obstinguished Name Individual Objects Object Groups DNS Server Group File List 		defaultDNSNameServerList					
		defaultDNS	Parameters				
		disableInspectProtocolList					
		dnsNameServerList					
		dnsParameters					
FlexConfig BelexConfig Object		eigrpAS					
Q Text Object		eigrpAuthKey					

Edit Text Object ?						
Name:	disableInspectProtocolList					
Description:	ist of protocols for which default inspections needs to be disabled. Default value is empty list. User must override this object to put values in this list.					
Variable Type	Multiple V Count 1					
	-					
1 esmtp						
Allow Overrides						
Override (0)						
	Save Cance	I				

Overview Analysis Policies Devices Objects AMP Intelligence Deploy Q System H4						
Device Management NAT VPN • QoS Platform Settings FlexConfig	Certificates			New Policy		
FlexConfig Policy	Domain	Status	Last Modified	and the second se		
at the cash	Global	Targeting 1 devices Up-to-date on all targeted devices	22210 127	Q. / 3		

inter Description			
Available FlexConfig C SlexConfig Object		Selected Prepend FlexConfigs	
×	#	Name	
Ser Defined	1	Default_Inspection_Protocol_Disable	
System Defined Default DNS_Configure	_		
Default_Inspection_Protocol_Disable			
Default_Inspection_Protocol_Enable			
DHCPv6_Prefix_Delegation_Configure			
DHCPv6_Prefix_Delegation_UnConfigure			
DNS_Configure			
DNS_UnConfigure			
Eigrp_Configure			
Eigrp_Interface_Configure			
Eigrp_UnConfigure			
Eigrp_Unconfigure_All			
Inspect_IPv6_Configure			
Inspect_IPv6_UnConfigure		Selected Append FlexConfigs	
ISIS_Configure			
ISIS_Interface_Configuration	*	Name	
ISIS_Unconfigure			
ISIS_Unconfigure_All			
Netflow_Add_Destination			
Mattlew Class Descentant	_		_

View FlexConfi	g Object						? ×		
Name:	Default_Inspection_Protocol_Disable								
Description:	Disable Default Inspection.								
🛕 Copy-pastir	△ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.								
🔘 Insert 💌					Deployment:	Once 🗸 Type:	Prepend 🗸		
<pre>class inspection_default #foreach (\$protocol in \$disableInspectProtocolList) #if(\$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST.contains(\$protocol)) no inspect \$protocol #end #end #end</pre>									
Variables									
Name		Dimension	Default Value	Property (Ty	Override	Description			
SYS_FW_ENABL	ED_INSPECT_PROTOCOL	MULTIPLE		SYSTEM	false				
disableInspectPr	otocolList	MULTIPLE	[esmtp]	FREEFORM:disa	false	List of protocols for wi	nich default		
							Close		

Targeted Devices		? ×
Targeted Devices		
Select devices to which you want to apply this policy. Available Devices	Selected Devices	
Search by name or value	Add to Policy	
	OK Cancel	

Disable ESMTP via FTD/ASA running FTD code Command Line Interface (CLI)

- 1. Login to FTD/ASA via CLI
- 2. Enter command 'configure inspection esmtp disable'
 - a. Note This will disable ESMTP inspection only on this device, if you are running FTD in HA or Cluster, please push the configuration thru FMC/FDM interface instead of CLI.
- 3. You can verify as mentioned above in verification section

