Configure BGP over Route-Based VPN on FTD Managed by FDM

Contents

Introduction
Prerequisites
Requirements
Components Used
<u>Configure</u>
Network Diagram
Configurations on VPN
Configurations on BGP
Verify
Troubleshoot

Introduction

This document describes configuring BGP over route-based site-to-site VPN on FTDv managed by FirePower Device Manager (FDM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of VPN
- BGP configurations on FTDv
- Experience with FDM

Components Used

The information in this document is based on these software and hardware versions:

- Cisco FTDv version 7.4.2
- Cisco FDM version 7.4.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Торо

Configurations on VPN

Step 1. Ensure the IP interconnectivity between nodes is ready and stable. The smart license on FDM is registered with the smart account successfully.

Step 2. The gateway of Site1 Client is configured with the inside IP address of Site1 FTD (192.168.70.1). The gateway of the Site2 client is configured with the inside IP address of Site2 FTD (192.168.50.1). Also, ensure the default route on both FTDs is configured correctly after FDM initialization.

 $Login \ to \ the \ GUI \ of \ each \ FDM. \ Navigate \ to \ Device > Routing \ . \ Click \ View \ Configuration \ . \ Click \ the \ Static \ Routing \ tab \ in \ order \ to \ verify \ the \ default \ static \ route.$

Firewall Device Manager Monitoring Policies	Objects Device: ftd	v742				admin Administra	ator v cisc	SECUR
Device Summary Routing								
Add Multiple Virtual Routers					~	>_ Commands ~	BGP Glo	obal Settings
Static Routing BGP OSPF EIGRP	ECMP Traffic Zones							
1 route					Filter			+
# NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP		SLA MONITOR	METRIC	ACTIONS
1 StaticRoute_IPv4	outside	IPv4	0.0.0/0	192.168.30.3			1	

Site1_FTD_Gateway

þ	Firewall Device Manager	Monitoring	Ø Policies	Objects	Device: ftdv742	_	\bigcirc			:	admin Administrato	r ×	cisco SECURE
	Device Summary Routing												
	Add Multiple Virtua	al Routers							~	>_ Cor	nmands 🗸	BGI	P Global Settings
	Static Routing BGP	OSPF E	IGRP	ECMP Traffic 2	Zones								
	1 route							T	Filter				+
	# NAME			INTER	FACE IP TY	PE NETWORKS	GATEWAY	'IP		SLA MO	NITOR	METRIC	ACTIONS
	1 StaticRoute_IPv4			outsi	ide IPv4	0.0.0.0/0) 192.16	8.10.3				1	

Site2_FTD_Gateway

Step 3. Configure route-based site-to-site VPN. In this example, first configure the Site1 FTD.

Step 3.1. Login to the FDM GUI of Site1 FTD. Create a new network object for the inside network of Site1 FTD. Navigate to Objects > Networks, click the + button.

Firewall Device Ma	anager Monitoring	Ø Policies	∷ Objects	Device: ftdv742	(\mathbf{b})		0	?	•	admin Administrator	~	cisco SEC	URE
∧ Object Types ←	1	Vetwork Ob	ojects ar	nd Groups									
C Networks	g	objects				T Filt	er					+	
S Ports					Pr	reset filter	rs: Syste	n deficed	User de	beob		\Box	

Create_Network_Object

Step 3.2. Provide necessary information. Click the ok button.

- Name: inside_192.168.70.0
- Type: Network
- Network: 192.168.70.0/24

Add Network Object	Ø	×
Name inside_192.168.70.0		
Description		
		li.
Type Network Host FQDN Range		
Network		
192.168.70.0/24 e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60		
CANCEL	ок	



Step 3.3. Navigate to Device > Site-to-Site VPN . Click View Configuration .

View Site-to-Site VPN

Step 3.4. Start to create a new site-to-site VPN. Click CREATE SITE-TO-SITE CONNECTION .

Firewall Device Manager	题 Monitoring	Policies	i≣ Objects	Device: ftdv742		6		?:	admin Administrator	cisco SEC	CURE
	Device Summa Site-to-S	iry Site VPN									
							T FB	ter			+
							Preset filte	rs: Route Based (VO).	Policy.Based		
	# NAME		LOCAL INT	RFACES	LOCAL NETWORKS	REMOTE NETWORKS	NAT EXEMPT			ACTIONS	
					There as	e no Site-to-Site connections yet.					
					Start by cre	ting the first Site-to-Site connection					
		CREATE SITE-TO-SITE CONNECTION									

Create_Site-to-Site_Connection

Step 3.5. Provide the necessary information.

- Connection Profile Name: Demo_S2S
- Type: Route Based (VTI)
- Local VPN Access Interface: click the dropdown list, then click Create new Virtual Tunnel Interface .



Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name	Туре
Demo_S2S	Route Based (VTI) Policy Based
Sites Configuration	
LOCAL SITE	REMOTE SITE
Local VPN Access Interface	Remote IP Address
Please select	*
T Filter	
	NEXT
Nothing found	
	~
Create new Virtual Tunnel Interface	

Create_VTI_in_VPN_Wizard

Step 3.6. Provide the necessary information in order to create a new VTI. Click the **OK** button.

- Name: demovti
- Tunnel ID: 1
- Tunnel Source: outside (GigabitEthernet0/0)
- IP Address And Subnet Mask: 169.254.10.1/24
- Status: click the slider to the Enabled position

Name demovti Most features work with named interfaces only, although some require unname	d interfaces.	
Description		h
Tunnel ID Tunnel Source Tunnel Source O - 10413	~	
IP Address and Subnet Mask 169.254.10.1 / 24 e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0		
	CANCEL	

Create_VTI_Details

Step 3.7. Continue to provide the necessary information. Click the **NEXT** button.

- Local VPN Access Interface: demovti (created in Step 3.6.)
- Remote IP Address: 192.168.10.1

New Site-to-site VPN	1 Endpoints	2 Configuration	3 Summary	
Local Network	FTDV742	VPN TUNNEL INTERNET	OUTSIDE	te Network
Identify the the Ic	interface on this device, and the re cal and remote networks that can	Define Endpoints emote peer's interface IP address, that use the connection, Traffic between th	form the point-to-point VPN connection. Then, ident ese networks is protected using IPsec encryption.	ăfy
	Connection Profile Name Demo_S2S		Type Route Based (VTI) Policy Based	
	Sites Configuration	REMOTE SITE		
	Local VPN Access Interface demovti (Tunnel1)	✓ Remote IP A 192.168. ⁻	uddress	
		CANCEL		

VPN_Wizard_Endpoints_Step1

Step 3.8. Navigate to IKE Policy. Click the **EDIT** button.

Firewall Device Manager Monitoring Policies Objects	Device: ftdv742	() () () () () () () () () () () () () (
New Site-to-site VPN	2 Configuration	3 Summary
Fin Local Network	VPN TUNNEL	OUTSICE
Select the Internet Key Exchange	Privacy Configuration (IKE) policy and enter the preshared keys needed to au IPsec proposals to use for encrypting traffic	thenticate the VPN connection. Then, select the c.
IKE Policy		
IKE policies are g connections.	obal, you cannot configure different policies per VPN. Any enable	Id IKE Policies are available to all VPN
IKE VERSION 2	IKE VERSION 1	
IKE Policy		
Globally applied	EDIT	
IPSec Proposal		
None selected	EDIT ()	

Edit_IKE_Policy

Step 3.9. For the IKE policy, you can use a pre-defined one or create a new one by clicking **Create New IKE Policy**.

In this example, toggle an existing IKE policy **AES-SHA-SHA** and also create a new one for demo purposes. Click the **OK** button in order to save.

- Name: AES256_DH14_SHA256_SHA256
- Encryption: AES, AES256
 DH Group: 14
- Integrity Hash: SHA, SHA256
- PRF Hash: SHA, SHA256
- Lifetime: 86400 (default)

		Add IKE v2 Policy	0 ×
▼ Filter		Priority 1 AES256_DH14_SHA256_SHA256	State
AES-GCM-NULL-SHA	0 ^	Encryption	
AES-SHA-SHA	0		~
DES-SHA-SHA	0		~
		Integrity Hash SHA × SHA256 × Pseudo Random Function (PRF) Hash	~
Create New IKE Policy	ок	Lifetime (seconds) 86400	
		Between 120 and 2147483647 seconds.	

CANCEL

Add_New_IKE_Policy

▼ Filter		
AES-GCM-NULL-SHA	0	^
AES-SHA-SHA	0	
DES-SHA-SHA	0	
AES256_DH14_SHA256_SHA256	0	
		~
Create New IKE Policy	ок)

Enable_New_IKE_Policy

Step 3.10. Navigate to the IPSec Proposal. Click the **EDIT** button.

Firewall Device Manager Monitoring	Policies Objects	Device: ftdv742		> 🖄 🗐 ?	° admin ° Administrator ✓	cisco SECURE
New Site-to-site VPN	1 Endpoints	2	Configuration	3 Summary		
C Local Network	FTDV742	VPN TUNNE	INTERNET	OUTSIDE	Ramote Network	
Selec	Then, select the					
	IKE Policy					
	IKE policies are glo connections.	bal, you cannot configure diff	erent policies per VPN. Any er	abled IKE Policies are available to all VPN		
	IKE VERSION 2		IKE VERSION 1 (
	IKE Policy					
	Globally applied	EDIT				
	IPSec Proposal					
	None selected	EDIT				

Edit_IKE_Proposal

Step 3.11. For the IPSec proposal, you can use a pre-defined or you can create a new one by clicking **Create new IPSec Proposal**. In this example, create a new one for demo purposes. Provide the necessary information. Click the **OK** button in order to save.

- Name: AES256_SHA256
- Encryption: AES, AES256
- Integrity Hash: SHA1, SHA256

	+			→ Add IKE v2 IPSec Proposal	0	×
	▼ Filter	SET DEFAULT		Name AES256_SHA256		
	AES-GCM in Default Set	0	^	Encryption		
VO	4ES-SHA	0	olicie	AES × AES256 ×		~
	des-SHA-1	0		Integrity Hash SHA1 × SHA256 ×		~
	Create new IPSec Proposal	NCEL OK	Ĭ	CANCEL	ОК	

Add_New_IPSec_Proposal

	+		
	▼ Filter	SET DEFAULT	
4	AES-GCM in Default Set	0	
, yo	AES-SHA	0	olicies
	DES-SHA-1	0	
	AES256_SHA256	0	
	Create new IPSec Proposal	CANCEL OK]

Enable_New_IPSec_Proposal

Step 3.12. Configure the pre-shared key. Click the **NEXT** button.

Note down this pre-shared key and configure it on the Site2 FTD later.

1	Firewall Device Manager	Monitoring	Policies	 Objects	Device: ftdv742		(>_)			?	:	admin Administrator	~	cisco	SECUR
				FTDV742		INTERNET		PEE	R ENDPO	INT					
					Pri	vacy Configura	ation								
		Se	lect the Intern	iet Key Exchang	e (IKE) policy and enter IPsec pro	the preshared keys nee posals to use for encryp	ded to authentica oting traffic.	ate the VP	N conne	ection. T	hen, se	elect the			
			IKE	Policy											
			0	IKE policies are of connections.	lobal, you cannot configure	e different policies per VPN.	Any enabled IKE Po	licies are a	wailable to	all VPN					
			IKE	/ERSION 2		IKE VERSI	ION 1								
			IKE	Policy											
			Glo	bally applied	EDIT										
			IPSe	ec Proposal											
			Cus	tom set selecte	d EDIT										
			Auth	nentication Type	ual Key O Certific	ate									
			Loc	al Pre-shared Ke											
			•												
			Rem	note Peer Pre-sh	ared Key										
			ŀ												
			19552	Prekty Blace		BACK									

Configure_Pre_Shared_Key

Step 3.13. Review the VPN configuration. If anything needs to be modified, click the **BACK** button. If everything is good, click the **FINISH** button.

demovti (169.254.10.1)
demovti (169.254.10.1)
aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256- sha,sha256-sha,sha256-14
aes,aes-256-sha-1,sha-256 Pre-shared Manual Key
28800 seconds
4608000 kilobytes
5
ed to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

VPN_Wizard_Complete

Step 3.14. Create an Access Control rule in order to allow traffic to pass through the FTD. In this example, allow all for demo purposes. Modify your policy based on your actual needs.

Security Po	olicies											
$\square \rightarrow \bigcirc$ ss	L Decryptic	on → ()	Identity \rightarrow \bigcirc) Security Intellige	nce 🔶 📀 N	NAT $ ightarrow$ \checkmark Acc	ess Control 🔿	Intrusion				
1 rule						1	Filter			<	× @. +	
		SOURCE			DESTINATION	DESTINATION						
# NAME		ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS		USERS	ACTIONS	
> 1 Demo_allow	Ð	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	% C.	

Access_Control_Rule_Example

Step 3.15. (Optional) Configure NAT exempt rule for the client traffic on FTD if dynamic NAT is configured for the client in order to access the internet. In this example, there is no need to configure a NAT-exempt rule because no dynamic NAT is configured on each FTD.

Step 3.16. Deploy the configuration changes.

Firewall Device Manager Monitoring Policies Obje	E Device: ftdv742				admin Administr	rator ~	cisco	SECURE
Device Summary Site-to-Site VPN								
1 connection profile				Filter Preset filters: Route Bas	+			
N NAME		LOCAL INTERFACES	LOCAL NETWORKS	REMOTE NETWORKS	NAT EXEMPT			ACTIONS
1 Demo_S2S	Route Based (VTI)	demovti					~	

Deploy_VPN_Configuration

Configurations on BGP

Step 4. Navigate to **Device > Routing**. Click **View Configuration**.



 $View_Routing_Configuration$

Step 5. Click the BGP tab and then click CREATE BGP OBJECT.

Firewall Device Manager	Monitoring F	Policies Objects	Device: ftdv742		0		?:	admin Administrator	 diala secure 	
Device Summary Routing										
Add Multiple Virtua	I Routers					~	>_ (Commands 🗸	BGP Global Settings	
Static Routing BGP	OSPF EIGRP	ECMP Traffic	Zones							
									+	
# NJ	AME	C	ESCRIPTION				ACTIONS			
			Th Start t	ere are no BGP objects yet. by creating the first BGP objec CREATE BCP OBJECT	rt.					
	Firewall Device Manager Device Summary Routing Add Multiple Virtue Static Routing BGP	Firewall Device Manager Monitoring Relations	Firewall Device Manager Image: Monitoring Policies Image: Objects Device Summary Routing Add Multiple Virtual Routers Static Routing BGP Static Routing BGP OSPF EIGRP ECMP Traffic	Firewall Device Manager Image: Monitoring Image: Objects Image: Device: ftdv742 Device Summary Routing Add Multiple Virtual Routers Add Multiple Virtual Routers Static Routing BGP OSPF EIGRP ECMP Traffic Zones	Firewall Device Manager Image: Monitoring Image: Monitoring Image: Monitoring Device Summary Routing Add Multiple Virtual Routers Static Routing BGP OSPF EGRP ECMP Traffic Zones Image: Monitoring Monitoring OSPF EIGRP ECMP Traffic Zones There are no BGP objects yet. Image: Monitoring Monitoring Monitoring CESCRPTION CESCRPTION Image: Monitoring Image: Monitoring There are no BGP objects yet. Start by creating the first BGP object Image: Monitoring Image: Monitoring Image: Monitoring Image: Monitoring Image: Monitoring	Firewall Device Manager Monitoring Policies Dig to Digieds Device: ftdv742 Device: ftdv742 Device Summary Routing Add Multiple Virtual Routers Static Routing BGP OSPF EGMP Composition There are no BGP objects yet. Static by creating the first BGP objects Creating the first BGP objects yet. Creating the first BGP objects	Firewall Device Manager Image: Monitoring Image: Objects Image:	Firewall Device Manager Monitoring Policies Device: ftdv742 Device Summary Routing Add Multiple Virtual Routers Static Routing OFF ECMP Traffic Zones Image: Constraint of the first BGP objects yet. Static Routing Image: Constraint of the first BGP objects yet. Image: Constraint of the first BGP obje	Firewall Device Manager Routing Policies Objects Device: ftdv7/22	Firewall Device Manager Image: State Routing BGP Commands Image: State Routing BGP Image: State Routing BGP Image: State Routing BGP Image: State Routing BGP Image: State Routing Image: State Routing Image: State Routing Image: State Routing Image: State Routing Image: State Routing Image: State Routing Image: State Routing Image: State Routing Image: State Routing Image: State Routing </td

Create_BGP_Object

Step 6. Provide the name of the object. Navigate to **Template** and configure. Click the **OK** button to save.

Name: demobgp

Line 1: Configure AS number. Click **as-number**. Manual input local AS number. In this example, AS number 65511 for Site1 FTD.

Line 2: Configure IP protocol. Click ip-protocol. Select ipv4.

Add New BGP Object	0 ×
Name demobgp	Description
Template 1 router bgp 65511 2 configure address-family ip-protocol v ipv4	Show disabled C Reset
ipv6	CANCEL OK

Create_BGP_Object_ASNumber_Protocol

Line 4: Configure more settings. Click settings, choose general, and then click Show disabled.

Add New BGP Object			0 ×
Name	Description		
demobgp			11.
Template		• Show disabled	🗘 Reset
I router bgp 65511			
2 configure address-family Address Family Address Family	IPV4 Settings		
⊖ 3 address-family ipv4 unicast			
••• 🗁 4 configure address-family ipv4	settings ~		
	general		
	advanced	CANCEL	ОК

Create_BGP_Object_AddressSetting

Line 6: Click the + icon in order to enable the line to configure the BGP network. Click **network-object**. You can see the existing available objects and choose one. In this example, choose the object name **inside_192.168.70.0** (created in Step 3.2.).

Add	Ne	w BGP Object 🔹 🖉 👋
Name		Description
demo	bgp	
Templat	te	🐼 Hide disabled 🗘 Rese
Θ	1	router bgp 65511
Θ	2	configure address-family ipv4~
Θ	3	address-family ipv4 unicast
Θ	4	configure address-family ipv4 general∽
Θ	5	distance bgp 20 200 200
⊙	6	network network-object ~
Ð	7	network network-object v route-map map-tag v
Ð	8	bgp inject-map inject-map 🗸 exist-map exist-map 🗸 options 🗸
€	9	configure aggregate-address map-type ~
€	10	configure filter-rules direction ~
€	11	configure neighbor neighbor-address remote-as as-number config-options v
⊙	12	configure ipv4 redistribution protocol v identifier none
⊙	13	bgp router-id router-id

Create_BGP_Object_Add_Network

Name	ban				Description								
denik	ngh									11.			
Templa	te							₩ Hide disabled	Φ	Reset			
Θ	1	router bgp 65511											
Θ	2	configure addr	configure address-family ipv4 ~										
Θ	з	address-fami	address-family ipv4 unicast										
Θ	4	IPV4 Network	IPV4 Network address										
Θ	5	distance	- 18P - 41	200 200									
••• O	6	network											
Ð	7	network				<u> </u>	^						
€	8	bgp inje	🕤 Outsid	elPv4DefaultRoute Net	work	0	otions						
⊙	9	configur	C Outsid	elPv4Gateway Host		6							
Ð	10	configur				<u> </u>							
€	11	configur	🕤 any-ip	v4 Network	8	0	mber	config-options 🗸					
Ð	12	configur	도 anv-in	v6 Network		6	none						
€	13	bgp router-i	Çi uny ip	O HOURSA		~							
			5	nside_192.168.70.0 N	etwork	Ð	~						
		L		insi	de_192.168.70.0								

Create_BGP_Object_Add_Network2

Line 11: Click the + icon in order to enable the line to configure the BGP neighbor-related information. Click **neighbor-address**, and manually input the peer BGP neighbor address. In this example, it is 169.254.10.2 (VTI IP address of Site2 FTD). Click **as-number**, and manually input the peer AS number. In this example, 65510 is for Site2 FTD. Click **config-options** and choose **properties**.

Name		Description	
demo	obgp		
Templa	te	Note that the two tests of the test of	
Θ	1	router bgp 65511	
Θ	2	configure address-family ipv4v	
Θ	3	address-family ipv4 unicast	
Θ	4	configure address-family ipv4 general ~	
Θ	5	distance bgp 20 200 200	
Θ	6	network inside_192.168.70.0 v	
Ð	7	network network-object v route-map map-tag v	
€	8	bgp inject-map inject-map ∨ exist-map exist-map ∨ options ∨	
Ð	9	configure aggregate-address map-type > Select Configuration Option	
€	10	configure filter-rules direction ~	
•••	11	configure neighbor 169.254.10.2 remote-as 65510 config-options -	
Ð	12	configure ipv4 redistribution protocol v identifier	
€	13	bgp router-id router-id	

Create_BGP_Object_NeighborSetting

Line 14: Click the + icon in order to enable the line to configure some properties of the neighbor. Click **activate-options** and choose **properties**.

Name		Description			
demo	obgp				
Templa	te	V Reset			
Θ	1	router bgp 65511			
Θ	2	configure address-family ipv4 ~			
Θ	3	address-family ipv4 unicast			
Θ	4	configure address-family ipv4 general ~			
Θ	5	distance bgp 20 200 200			
Θ	6	network inside_192.168.70.0 v			
€	7	network network-object v route-map map-tag v			
€	8	bgp inject-map inject-map 🗸 exist-map exist-map 🗸 options 🗸			
€	9	configure aggregate-address map-type v			
€	10	configure filter-rules direction ~			
Θ	11	configure neighbor 169.254.10.2 remote-as 65510 properties v			
Θ	12	neighbor 169.254.10.2 remote-as Select Configuration Option			
€	13	configure neighbor 169.254.10.2 Gemote-as-settingsv			
Θ	14	configure neighbor 169.254.10.2 activate activate-options			
€	15	configure ipv4 redistribution protocol v ide properties			
€	16	bgp router-id			

 $Create_BGP_Object_NeighborSetting_Properties$

Line 13: Click the + icon in order to enable the line to show advanced options. Click **settings** and choose **advanced**.

Name		Description		
dem	obgp			
Templa	ate	We disabled ↓ Reset		
Θ	1	router bgp 65511		
Θ	2	configure address-family ipv4 ~		
Θ	з	address-family ipv4 unicast		
Θ	4	configure address-family ipv4 general∽		
Θ	5	distance bgp 20 200 200		
Θ	6	network inside_192.168.70.0 v		
€	7	network network-object v route-map map-tag v		
€	8	<pre>bgp inject-map inject-map ~ exist-map exist-map ~ options ~</pre>		
€	9	configure aggregate-address map-type v		
€	10	configure filter-rules direction ~		
Θ	11	configure neighbor 169.254.10.2 Select Neighbor Settings		
Θ	12	neighbor 169.254.10.2 remote-as 65510		
••• ⊙	13	configure neighbor 169.254.10.2 remote-as settings v		
Θ	14	configure neighbor 169.254.10.2 activate general		
Θ	15	neighbor 169.254.10.2 activate		
€	16	configure neighbor 169.254.10.2 activate advanced		
€	17	configure ipv4 redistribution protocol v iden		
€	18	bgp router-id migration		
		ha-mode		
		CANCEL OK		

Create_BGP_Object_NeighborSetting_Properties_Advanced

Line 18: Click options and choose disable in order to disable path MTU discovery.

Name		Description		
demo	obgp			
Templa	te	🐼 Hide disabled 🗘 Reset		
Θ	1	router bgp 65511		
Θ	2	configure address-family ipv4 ~		
Θ	з	address-family ipv4 unicast		
Θ	4	configure address-family ipv4 general∨		
Θ	5	distance bgp 20 200 200		
Θ	6	network inside_192.168.70.0 v		
€	7	network network-object v route-map map-tag v		
€	8	bgp inject-map inject-map v exist-map exist-map v options v		
€	9	configure aggregate-address map-type ~		
€	10	configure filter-rules direction ~		
Θ	11	configure neighbor 169.254.10.2 remote-as 65510 properties 🗸		
Θ	12	neighbor 169.254.10.2 remote-as 65510		
Θ	13	configure neighbor 169.254.10.2 remote-as advanced v		
Θ	14	neighbor 169.254.10.2 password secret ∨		
Θ	15	configure neighbor 169.254.10.2 hops options v		
Θ	16	neighbor 169.254.10.2 version version optional)		
Θ	17	neighbor 169.254.10.2 transport connection-mode options		
Θ	18	neighbor 169.254.10.2 transport path-mtu-discovery options v		
Θ	19	configure neighbor 169.254.10.2 activate properties		
Θ	20	neighbor 169.254.10.2 activate disable		
€	21	configure neighbor 169.254.10.2 activate settings		
Ð	22	configure ipv4 redistribution protocol v identifier none		
€	23	bgp router-id router-id		

 $Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD$

Line 14, 15, 16, 17: Click the **-** button in order to disable the lines. Then, click the **OK** button to save the BGP object.

Name		Description			
demobgp					
Templat	e	🐼 Hide disabled 🗘 Reset			
Θ	1	router bgp 65511			
Θ	2	configure address-family ipv4 v			
Θ	3	address-family ipv4 unicast			
Θ	4	configure address-family ipv4 general v			
Θ	5	distance bgp 20 200 200			
Θ	6	<pre>network inside_192.168.70.0 v</pre>			
⊙	7	network network-object v route-map map-tag v			
⊙	8	<pre>bgp inject-map inject-map ~ exist-map exist-map ~ options ~</pre>			
⊙	9	configure aggregate-address map-type v			
⊙	10	configure filter-rules direction v			
Θ	11	configure neighbor 169.254.10.2 remote-as 65510 properties v			
Θ	12	neighbor 169.254.10.2 remote-as 65510			
Θ	13	configure neighbor 169.254.10.2 remote-as advanced v			
Θ	14	neighbor 169.254.10.2 password secret 🗸			
Θ	15	configure neighbor 169.254.10.2 hops options∽			
Θ	16	neighbor 169.254.10.2 version version-number			
Θ	17	neighbor 169.254.10.2 transport connection-mode options v			
Θ	18	neighbor 169.254.10.2 transport path-mtu-discovery disable v			
Θ	19	configure neighbor 169.254.10.2 activate properties v			
Θ	20	neighbor 169.254.10.2 activate			
•	21	configure neighbor 169.254.10.2 activate settings v			
•	22	configure 1pv4 redistribution protocol v identifier none			
	23	bgp router-1d router-1d			
		CANCEL OK			

Create_BGP_Object_DisableLines

This is an overview of the BGP setting in this example. You can configure the other BGP settings based on your actual needs.

Name	Description	
demobap		

Templat	te	We disabled ↓ Reset
Θ	1	router bgp 65511
Θ	2	configure address-family ipv4v
Θ	з	address-family ipv4 unicast
Θ	4	configure address-family ipv4 general v
Θ	5	distance bgp 20 200 200
Θ	6	network inside_192.168.70.0 ~
€	7	network network-object v route-map map-tag v
€	8	bgp inject-map inject-map v exist-map exist-map v options v
€	9	configure aggregate-address map-type ~
€	10	configure filter-rules direction v
Θ	11	configure neighbor 169.254.10.2 remote-as 65510 properties v
Θ	12	neighbor 169.254.10.2 remote-as 65510
Θ	13	configure neighbor 169.254.10.2 remote-as advanced v
€	14	neighbor 169.254.10.2 password secret
€	15	configure neighbor 169.254.10.2 hops options v
€	16	neighbor 169.254.10.2 version version-number
€	17	neighbor 169.254.10.2 transport connection-mode options v
Θ	18	neighbor 169.254.10.2 transport path-mtu-discovery disable v
Θ	19	configure neighbor 169.254.10.2 activate properties
Θ	20	neighbor 169.254.10.2 activate
€	21	configure neighbor 169.254.10.2 activate settings v
€	22	configure ipv4 redistribution protocol v identifier none
€	23	bgp router-id

	CANCEL	ОК
Create_BGP_Object_Final_Overview		

Step 7. Deploy the BGP configuration changes.

Firew	vall Device Manager Monitoring	Image: Second	(C)
	Device Summary Routing		
	Add Multiple Virtual Routers		✓ ➤ Commands ✓ BGP Global Settings
	Static Routing BGP OSPF	EIGRP ECMP Traffic Zones	
	1 object		+
	II NAME	DESCRIPTION	ACTIONS
	1 demobgp		

Deploy_BGP_Configuration

Step 8. Now the configuration for Site1 FTD is completed.

In order to configure Site2 FTD VPN and BGP, repeat Step 3. to Step 7. with corresponding parameters of Site2 FTD.

Configuration overview of Site1 FTD and Site2 FTD in CLI.

NGFW Version 7.4.2 NGFW Version 7.4.2 interface GigabitEthernet0/0 interface GigabitEthernet0/0 nameif outside cts manual propagate sgt disabled trusted propagate sgt disabled trusted security-level 0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside security-level 0 ip address 192.168.70.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside security-level 0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovi 25 paddress 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovi 1 nameif demovi 25 ip address 192.168.70.1 255.255.255.0 interface outside tunnel source interface outside tunnel source interface outside tunnel source interface outside tunnel source interface outside tunnel odo ipsec ipv4 tunnel mode ipsec ipv4 tunnel outsidePV-QNBOX_ACL remark rule-id 268435457: ACCESS POILCY: NGFW_Access_Policy access-rist NGFW_ONBOX_ACL remark rule-id 268435457: L5 access-rist NGFW_ONBOX_ACL remark rule-id 268435457: L5 access-rist NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Findi	Site1 FTD	Site2 FTD
NGFW Version 7.4.2 interface GigabitEthemet0/0 interface GigabitEthemet0/0 nameif outside cs manual propagate sgt preserve-untag propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthemet0/2 nameif inside security-level 0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthemet0/2 nameif inside security-level 0 ip address 192.168.50.1 255.255.255.0 interface Tunnel1 nameif domovt125 interface Tunnel1 nameif domovt25 ip address 192.2168.70.1 255.255.255.0 unnel source interface outside unnel destination 192.168.30.1 tunnel destination 192.168.30.1 unnel protection ipsec profile psec_profile/e4084d322d object network inside_192.168.30.3 object network NutsideIPV4Gateway host 192.168.30.3 bost 192.168.30.3 object network inside_192.168.70.0 subset 192.168.30.3 cccess-fils NGFW_ONBOX_ACL remark rule-id 268435457: 1.5 RCLES POLLCY: NGFW_Access_Policy access-fils NGFW_ONBOX_ACL remark rule-id 268435458: 1.5 RULE: Inside_Outside_RW_ONBOX_ACL remark rule-id 268435458: 15 RULE: Sils NGFW_ONBOX_ACL remark rule-id 26843545		NGFW Version 7.4.2
interface GigabitEthernet0/0 anneif outside cs manual propagate sgt preserve-untag propagate sgt preserve-untag propagate sgt preserve-untag propagate sgt freserve-untag propagate sgt freser	NGFW Version 7.4.2	
nameri outside cis manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 mameri inside security-level 0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 mameri inside security-level 0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameri demovti p address 192.168.70.1 255.255.255.0 interface Tunnel1 nameri destination 192.168.70.0 subnet 192.168.70.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.2	interface GigabitEthernet0/0	interface GigabitEthernet0/0
animula cis manual propagate set preserve-unitig propagate set preserve-unitig policy static set disabled trusted security-level 0 security-level 0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet02 nameif inside security-level 0 ip address 192.168.70.1 255.255.255.0 interface GigabitEthernet02 nameif inside security-level 0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovit25 ip address 192.254.10.1 255.255.255.0 interface outside tunnel source interface outside tunnel source interface outside tunnel source interface outside tunnel source interface outside tunnel source interface outside tunnel destination 192.168.70.1 tunnel orotecin ipsec profile ipsec_profile/e4084d322d object network OutsidelPv4Gateway host 192.168.70.0 255.255.255.0 submet 192.168.0.0 subst 192.168.70.0 255.255.255.0 submet 192.168.0.0 255.255.255.0 access-sits NGFW_ONBOX_ACL global access-sits NGFW_ONBOX_ACL remark rule-id 268435457: tc access-sits NGFW_ONBOX_ACL solvanced trust object-group access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside any rule-id 268435458: L5	nameif outside	nameif outside
rest mannarie propagate sgl preserve-uning propagate sgl preserve-uning policy static sgt disabled trusted security-level 0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside security-level 0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside security-level 0 ip address 192.168.50.1 255.255.255.0 interface Tunnel1 nameif demovi25 interface Tunnel1 nameif demovi25 interface Tunnel1 nameif demovi25 ip address 169.254.10.1 255.255.255.0 tunnel source interface outside tunnel destination 192.168.30.1 tunnel destination 192.168.30.1 unnel mode ipsec ipv4 tunnel protection ipsec profile/e4084d322d object network OutsideIPv4Gateway host 192.168.70.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.50.0 255.255.255.0 access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: D	cts manual	cts manual
propository static signt disabled trusted security-level 0 security-level 0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 interface GigabitEthernet0/2 nameif inside security-level 0 iscurity-level 0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif inside interface Tunnel1 nameif demovti ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti ip address 192.168.10.1 unnel source interface outside tunnel source interface outside tunnel destination 192.168.10.1 tunnel source interface outside unnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile/e4084d322d object network OutsideIPv4Gateway host 192.168.70.0 host 192.168.70.0 255.255.255.0 subnet 192.168.50.0 255.255.255.0 sccess-sits NGFW_ONBOX_ACL remark rule-id 268435457: L5 acccess-group NGFW_ONBOX_ACL advanced trust object-group access-sits NGFW_ONBOX_ACL advanced trust object-group access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Inside_Outside_RV_ONBOX_ACL remark rule-id 268435458: L5 access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Dano_allow access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS <td>nronagate sof preserve-untag</td> <td>propagate sgt preserve-untag</td>	nronagate sof preserve-untag	propagate sgt preserve-untag
 printy andre sgrunty-level 0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif imside security-level 0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti ip address 169.254.10.1 255.255.255.0 interface Tunnel1 nameif demovti ip address 169.254.10.1 255.255.255.0 interface Tunnel1 nameif demovti ip address 169.254.10.1 255.255.255.0 interface Tunnel1 nameif demovi1 ip address 169.254.10.1 255.255.255.0 interface Tunnel1 nameif demovi2 ip address 169.254.10.2 255.255.0 interface Tunnel1 nameif demovi1 ip address 169.254.10.2 255.255.0 inturnel osurce interface outside tunnel source interface outside tunnel mode ipsec ipv4 tunel destination 192.168.50.0 subnet 192.168.70.0 subnet 192.168.7	policy static set disabled trusted	policy static sgt disabled trusted
 Junterface GigabitEthermet0/2 Interface GigabitEthermet0/2 Interface GigabitEthermet0/2 Interface GigabitEthermet0/2 Interface GigabitEthermet0/2 Interface Tunnel1 Intefface Tunnel	socurity level 0	security-level 0
interface GigabitEthernet0/2 nameif inside security-level 0 ip address 192,168.70.1 255.255.255.0 interface Tunnel1 nameif demovti p address 192,168.70.1 255.255.255.0 interface Tunnel1 nameif demovti p address 192,168.70.1 255.255.255.0 interface Tunnel1 nameif demovti25 ip address 169.254.10.2 255.255.255.0 tunnel source interface outside tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile/e4084d322d object network OutsideIPv4Gateway host 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL remark rule-id 268435457: RULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 268435457: RULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 268435458: IS NGFW_ONBOX_ACL remark rule-id 268435458: POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: LS RULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 1: LS RULE: DefaultActionRule	ip address 192.168.30.1 255.255.255.0	ip address 192.168.10.1 255.255.255.0
interface GigabitEthernet0/2 namefi inside security-level 0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 namefi demovti ip address 192.168.70.1 255.255.255.0 interface Tunnel1 namefi demovti ip address 192.168.70.1 255.255.255.0 tunnel source interface outside tunnel source interface outside tunnel source interface outside tunnel source interface outside tunnel ode ipsec ipv4 tunnel mode ipsec ipv4 tunnel mode ipsec profile ipsec_profile/e4084d322d object network OutsideIPv4Gateway host 192.168.70.0 subnet 192.168.70.0		interface GigabitEthernet0/2
nameif inside security-level 0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti ja address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti ja address 192.254.10.1 255.255.255.0 tunnel source interface outside tunnel source interface outside tunnel source interface outside tunnel destination 192.168.10.1 tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile jese_profile je4084d322d object network OutsideIPv4Gateway host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 access-list NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group access-list NGFW_ONBOX_ACL remark rule-id 268435458: RULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 268435458: RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group access-list NGFW_ONBOX_ACL advanced permit object-group access-list NGFW_ONBOX_ACL advanced permit object-group access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	interface GigabitEthernet0/2	nameifinside
security-level 0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti in definess 169.254.10.2 255.255.255.0 tunnel source interface outside tunnel destination 192.168.10.1 tunnel mode ipsee ipv4 tunnel mode ipsee profile ipsec_profile/e4084d322d object network OutsideIPv4Gateway host 192.168.30.3 object network OutsideIPv4Gateway host 192.168.30.3 object network OutsideIPv4Gateway host 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL remark rule-id 268435458: RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL remark rule-id 268435458: RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL remark rule-id 268435458: RULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 268435458: RULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: POLICY: NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	nameif inside	security-level 0
ip address 192.168.70.1 255.255.255.0 interface Tunnell nameif demovti ip address 169.254.10.1 255.255.255.0 tunnel source interface outside tunnel destination 192.168.10.1 tunnel destination 192.168.30.1 tunnel protection ipsec profile/e4084d322d object network OutsideIPv4Gateway host 192.168.30.3 object network outsideIPv4Gateway host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 access-list NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL advanced trust object-group [acSveg-268435457 ifc inside any ifc outside any rule-id 268435457 vent-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: CRULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL remark rule-id 268435458: CCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: CRULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-	security-level 0	ip address 192.168.50.1 255.255.255.0
interface Tunnel1 nameif demovti ip address 169.254.10.1 255.255.255.0 tunnel source interface outside tunnel source interface outside tunnel source interface outside tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile/e4084d322d object network OutsideIPv4Gateway host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 access-list NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_ONBOX_ACL remark rule-id 268435458: L5 RULE: Inside_ONBOX_ACL advanced trust object-group access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group access-list NGFW_	ip address 192.168.70.1 255.255.255.0	
interface Tunnel1 nameif demovti25 ip address 169.254.10.2 55.255.05.0 tunnel source interface outside tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile e4084d322d object network OutsideIPv4Gateway host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: IX NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL advanced permit object-group acsvcg-268435457 if inside any rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_		interface Tunnel1
nameif demovtiip address 169.254.10.2 255.255.0ip address 169.254.10.1 255.255.255.0tunnel source interface outsidetunnel source interface outsidetunnel source interface outsidetunnel source interface outsidetunnel destination 192.168.30.1tunnel mode ipsec ipv4tunnel protection ipsec profile ipsec_profile/e4084d322dobject network OutsideIPv4Gatewayhost 192.168.30.3object network inside_192.168.70.0subnet 192.168.50.0subnet 192.168.70.0subnet 192.168.50.0access-ist NGFW_ONBOX_ACL globalaccess-list NGFW_ONBOX_ACL globalaccess-list NGFW_ONBOX_ACL remark rule-id 268435457:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL advanced trust object-groupaccess-list NGFW_ONBOX_ACL advanced trust object-groupaccess-list NGFW_ONBOX_ACL advanced permit object-groupaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSACCESS POLICY: NGFW_Access_Policyacce	interface Tunnel1	nameif demovti25
ip address 169.254.10.1 255.255.0 tunnel source interface outside tunnel destination 192.168.10.1 tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile/e4084d322d object network outsideIPv4Gateway host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 access-list NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group lacSvcg-268435457 ic inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule pefaultActionRule	nameif demovti	ip address 169.254.10.2 255.255.255.0
tunnel source interface outside tunnel destination 192.168.30.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile e4084d322d object network OutsideIPv4Gateway host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.50.0 255.255.255.0 subnet 192.168.50.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.50.0 255.255.255.0 subnet 192.168.70.0 SUC_ACL genark rule-id 268435457: L5 RULE: Inside_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark	ip address 169.254.10.1 255.255.255.0	tunnel source interface outside
tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile/e4084d322d object network OutsideIPv4Gateway host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 subnet 192.168.70.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: RULE: Inside_Outside_any ifc outside any ule-id 268435457 ifc inside any ifc outside any rule-id 268435457 ifc inside any ifc outside any rule-id 268435457 ifc inside any ifc outside any rule-id 268435457 ic inside any ifc outside any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	tunnel source interface outside	tunnel destination 192.168.30.1
tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile/e4084d322d object network OutsideIPv4Gateway host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_ACcess_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RCCESS POLICY: NGFW_ACCESS_POLICY access-list NGFW_ONBOX_ACL advanced trust object-group lacSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RCCESS POLICY: NGFW_ACCESS_POLICY access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	tunnel destination 192.168.10.1	tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec_profile ide084d322d object network OutsideIPv4Gateway host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 uccess-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group lacSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_ACCESS_POlicy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	tunnel mode ipsec ipv4	tunnel protection ipsec profile ipsec_profile e4084d322d
object network OutsideIPv4Gatewayobject network OutsideIPv4Gatewayhost 192.168.30.3object network inside_192.168.70.0subnet 192.168.70.0subnet 192.168.70.0subnet 192.168.70.0subnet 192.168.50.0access-group NGFW_ONBOX_ACL globalaccess-group NGFW_ONBOX_ACL globalaccess-list NGFW_ONBOX_ACL remark rule-id 268435457:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435457:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL advanced trust object-groupacsvcg-268435457 ifc inside any ifc outside any rule-id268435457 event-log bothaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL advanced permit object-groupaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-i	tunnel protection ipsec profile ipsec_profile e4084d322d	
object network OutsideIPv4Gatewayhost 192.168.10.3host 192.168.30.3object network inside_192.168.70.0object network inside_192.168.70.0subnet 192.168.50.0subnet 192.168.70.0 255.255.255.0subnet 192.168.50.0access-group NGFW_ONBOX_ACL globalaccess-group NGFW_ONBOX_ACL remark rule-id 268435457:access-list NGFW_ONBOX_ACL remark rule-id 268435457:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435457:LSRULE: Inside_Outside_Ruleaccess-list NGFW_ONBOX_ACL advanced trust object-groupaccess-list NGFW_ONBOX_ACL advanced trust object-groupacsvcg-268435457 ifc inside any ifc outside any rule-id268435457 event-log bothaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS <td></td> <td>object network OutsideIPv4Gateway</td>		object network OutsideIPv4Gateway
host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group lacSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	object network OutsideIPv4Gateway	host 192.168.10.3
object network inside_192.168.70.0subnet 192.168.70.0 255.255.255.0subnet 192.168.70.0 255.255.255.0subnet 192.168.70.0 255.255.255.0success-group NGFW_ONBOX_ACL globalaccess-list NGFW_ONBOX_ACL remark rule-id 268435457:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL advanced trust object-groupacsvcg-268435457 ifc inside any ifc outside any rule-id268435457 event-log bothaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1268435458:LS RULE: Demo_allowaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: LS RULE:DefaultActionRuleDefaultActionRule	host 192.168.30.3	object network inside_192.168.50.0
subnet 192.168.70.0 255.255.0 access-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group lacSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	object network inside_192.168.70.0	subnet 192.168.50.0 255.255.255.0
access-group NGFW_ONBOX_ACL global access-group NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	subnet 192.168.70.0 255.255.255.0	
access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group lacSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule		access-group NGFW_ONBOX_ACL global
access-list NGFW_ONBOX_ACL remark rule-id 268435457:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435457:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL advanced trust object-groupaccess-list NGFW_ONBOX_ACL advanced trust object-grouplacSvcg-268435457 ifc inside any ifc outside any rule-id268435457 event-log bothaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:268435457 event-log bothaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:268435457 event-log bothaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL advanced permit object-groupaccess-list NGFW_ONBOX_ACL advanced permit object-grouplacSvcg-268435458 any any rule-id 268435458 event-log bothaccess-list NGFW_ONBOX_ACL advanced permit object-grouplacSvcg-268435458 any any rule-id 268435458 event-log bothaccess-list NGFW_ONBOX_ACL advanced permit object-grouplacSvcg-268435458 any any rule-id 268435458 event-log bothaccess-list NGFW_ONBOX_ACL advanced permit object-grouplacSvcg-268435458 any any rule-id 268435458 event-log bothaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE:DefaultActionRuleaccess-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE:	access-group NGFW_ONBOX_ACL global	access-list NGFW_ONBOX_ACL remark rule-id 268435457:
ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435457: L5RULE: Inside_Outside_Ruleaccess-list NGFW_ONBOX_ACL advanced trust object-grouplacSvcg-268435457 ifc inside any ifc outside any rule-id268435457 event-log bothaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_ONBOX_ACL advanced permit object-groupaccess-list NGFW_ONBOX_ACL advanced permit object-groupaccess-list NGFW_ONBOX_ACL advanced permit object-groupaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE:DefaultActionRule	access-list NGF w_ONBOA_ACL remark rule-id 208435457:	ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435457RULE: Inside_Outside_RuleRULE: Inside_Outside_Ruleaccess-list NGFW_ONBOX_ACL advanced trust object-groupaccess-list NGFW_ONBOX_ACL advanced trust object-groupaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435458access-list NGFW_ONBOX_ACL remark rule-id 268435458:RULE: Demo_allowaccess-list NGFW_ONBOX_ACL advanced permit object-groupaccess-list NGFW_ONBOX_ACL advanced permit object-groupaccess-list NGFW_ONBOX_ACL advanced permit object-groupaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE:DefaultActionRuleaccess-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE:DefaultActionRuleaccess-list NGFW_ONBOX_ACL advanced denv in anv anv	ACCESS POLICY: NGFW_ACCESS_POlicy	access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5
ROLE. Iniside_Outside_Kuleaccess-list NGFW_ONBOX_ACL advanced trust object-grouplacSvcg-268435457 ifc inside any ifc outside any rule-id268435457 event-log bothaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:ACCESS POLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 268435458:LE: Demo_allowaccess-list NGFW_ONBOX_ACL advanced permit object-grouplacSvcg-268435458 any any rule-id 268435458 event-log bothaccess-list NGFW_ONBOX_ACL remark rule-id 1: ACCESSPOLICY: NGFW_Access_Policyaccess-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE:DefaultActionRule	access-list NGF w_ONBOA_ACL remark rule-lu 208453457: L5	RULE: Inside_Outside_Rule
access-list NOFW_ONBOX_ACL advanced thust object-group [acSvcg-268435457 ifc inside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group [acSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group [acSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group [acSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRuleacvess-list NGFW_ONBOX_ACL advanced denv in any any	ROLE. Inside_Outside_Kule	access-list NGFW_ONBOX_ACL advanced trust object-group
268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	access-list NOT w_ONBOA_ACL advanced trust object-group	acSvcg-268435457 ifc inside any ifc outside any rule-id
access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	268435457 event-log both	268435457 event-log both
ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	access-list NGEW ONBOX ACL remark rule_id 268435458	access-list NGFW_ONBOX_ACL remark rule-id 268435458:
access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	ACCESS POLICY: NGEW Access Policy	ACCESS POLICY: NGFW_Access_Policy
RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5	access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5
access-list NGFW_ONBOX_ACL advanced permit object-group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule DefaultActionRule	RULE: Demo allow	RULE: Demo_allow
acSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	access-list NGFW ONBOX ACL advanced permit object-group	access-list NGF w_ONBOX_ACL advanced permit object-group
access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule DefaultActionRule	acSvcg-268435458 any any rule-id 268435458 event-log both	acsives-200455456 any any full-full 200455456 event-fog both
POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule DefaultActionRule	access-list NGFW ONBOX ACL remark rule-id 1: ACCESS	DOLICY: NGEW Access Doligy
access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	POLICY: NGFW_Access Policy	access_list NGEW ONROY ACL remark rule id 1.15 DULE.
DefaultActionRule access_list NGEW_ONROX_ACL advanced denv in any any	access-list NGFW ONBOX ACL remark rule-id 1: L5 RULE:	Default Action Pule
	DefaultActionRule	access-list NGEW ONBOX ACL advanced denv in any any

	1
access-list NGFW_ONBOX_ACL advanced deny ip any any	rule-id 1
rule-id 1	
	router bgp 65510
router bgp 65511	bgp log-neighbor-changes
bgp log-neighbor-changes	bgp router-id vrf auto-assign
bgp router-id vrf auto-assign	address-family ipv4 unicast
address-family ipv4 unicast	neighbor 169.254.10.1 remote-as 65511
neighbor 169.254.10.2 remote-as 65510	neighbor 169.254.10.1 transport path-mtu-discovery disable
neighbor 169.254.10.2 transport path-mtu-discovery disable	neighbor 169.254.10.1 activate
neighbor 169.254.10.2 activate	network 192.168.50.0
network 192.168.70.0	no auto-summary
no auto-summary	no synchronization
no synchronization	exit-address-family
exit_address_family	
exit-address-ranning	route outside $0.0.0.0.0.0.1921681031$
route outside 0.0.0.0.0.0.0.102 168 30.2.1	1000 000300 0.0.0.0 0.0.0.0 192.108.10.5 1
route outside 0.0.0.0 0.0.0.0 192.108.30.3 1	ammta ingga ikaw2 ingga managal AES256 SUA256
	crypto ipsec ikev2 ipsec-proposal AES256_SHA256
crypto ipsec ikev2 ipsec-proposal AES256_SHA256	protocol esp encryption aes-256 aes
protocol esp encryption aes-256 aes	protocol esp integrity sha-256 sha-1
protocol esp integrity sha-256 sha-1	
	crypto ipsec profile ipsec_profile e4084d322d
crypto ipsec profile ipsec_profile e4084d322d	set ikev2 ipsec-proposal AES256_SHA256
set ikev2 ipsec-proposal AES256_SHA256	set security-association lifetime kilobytes 4608000
set security-association lifetime kilobytes 4608000	set security-association lifetime seconds 28800
set security-association lifetime seconds 28800	
	crypto ipsec security-association pmtu-aging infinite
crypto ipsec security-association pmtu-aging infinite	
	crypto ikev2 policy 1
crypto ikev2 policy 1	encryption aes-256 aes
encryption aes-256 aes	integrity sha256 sha
integrity sha256 sha	group 14
group 14	prf sha256 sha
prf sha256 sha	lifetime seconds 86400
lifetime seconds 86400	
	crypto ikey2 policy 20
crypto ikey? policy 20	encryption aes-256 aes-192 aes
encryption aes_256 aes_192 aes	integrity sha512 sha384 sha256 sha
integrity sha512 sha384 sha256 sha	group 21 20 16 15 14
aroup 21 20 16 15 14	prf sha512 sha384 sha256 sha
prf sha512 sha284 sha256 sha	lifetime seconds 86400
lifetime seconds 86400	incline seconds 80400
ineume seconds 86400	amonto ileas 2 anable anto ide
	crypto ikev2 enable outside
crypto ikev2 enable outside	
	group-policy s2sGP 192.168.30.1 internal
group-policy s2sGP 192.168.10.1 internal	group-policy s2sGP 192.168.30.1 attributes
group-policy s2sGP 192.168.10.1 attributes	vpn-tunnel-protocol ikev2
vpn-tunnel-protocol ikev2	
	tunnel-group 192.168.30.1 type ipsec-121
tunnel-group 192.168.10.1 type ipsec-121	tunnel-group 192.168.30.1 general-attributes
tunnel-group 192.168.10.1 general-attributes	default-group-policy s2sGP 192.168.30.1
default-group-policy s2sGP 192.168.10.1	
	tunnel-group 192.168.30.1 ipsec-attributes
tunnel-group 192.168.10.1 ipsec-attributes	ikev2 remote-authentication pre-shared-key *****
ikev2 remote-authentication pre-shared-key *****	ikev2 local-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****	
	1

Verify

Use this section in order to confirm that your configuration works properly.

Step 1. Navigate to the CLI of each FTD via console or SSH in order to verify the VPN status of phase 1 and phase 2 through the commands **show crypto ikev2 sa** and **show crypto ipsec sa**.

Site1 FTD	Site2 FTD
ftdv742# show crypto ikev2 sa	
IKEv2 SAs:	ftdv742# show crypto ikev2 sa
Session-id:134, Status:UP-ACTIVE, IKE count:1, CHILD count:1	IKEv2 SAs:
Tunnel-id Local Remote fvrf/ivrf Status Role	Session-id:13, Status:UP-ACTIVE, IKE count:1, CHILD count:1
563984431 192.168.30.1/500 192.168.10.1/500 Global/Global READY RESPONDER	Tunnel-id Local Remote fvrf/ivrf Status Role 339797985 192.168.10.1/500 192.168.30.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	Global/Global READY INITIATOR Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/5145 sec	Life/Active Time: 86400/74099 sec Child sa: local selector 0.0.0.0/0 -
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535	255.255.255.255/65535 remote selector 0.0.0.0/0 - 255.255.255.255/65535 ESP spi in/out: 0xb7b5b38b/0xf0c4239d
remote selector 0.0.0.0/0 - 255.255.255.255/65535	
ESP spi in/out: 0xf0c4239d/0xb7b5b38b	
ftdv742# show crypto ipsec sa	ftdv742# show crypto ipsec sa
interface: demovti Crypto map tag:vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1	interface: demovti25 Crypto map tag:vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.10.1
Protected vrf (ivrf): Global local ident (addr/mask/prot/port): (0.0.0/0/0.0.0/0/0)	Protected vrf (ivrf): Global local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0/0.0.0/0/0) current_peer: 192.168.10.1	remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.30.1
 #pkts encaps: 5720, #pkts encrypt: 5720, #pkts digest: 5720 #pkts decaps: 5717, #pkts decrypt: 5717, #pkts verify: 5717 	<pre>#pkts encaps: 5721, #pkts encrypt: 5721, #pkts digest: 5721 #pkts decaps: 5721, #pkts decrypt: 5721, #pkts verify: 5721</pre>
<pre>#pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 5720, #pkts comp failed: 0,</pre>	<pre>#pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 5721, #pkts comp failed: 0,</pre>

#pkts decomp failed: 0	#pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0,	<pre>#pre-frag successes: 0, #pre-frag failures: 0,</pre>
#fragments created: 0	#fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated	#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated
frgs needing reassembly: 0	frgs needing reassembly: 0
#TFC rcvd: 0. #TFC sent: 0	#TFC rcvd: 0. #TFC sent: 0
#Valid ICMP Errors revd: 0 #Invalid ICMP Errors	#Valid ICMP Errors revd: 0 #Invalid ICMP Errors
revd: 0	revd: 0
the and arrors: 0 throad arrors: 0	the and arrors: 0 throat arrors: 0
local crypto endpt : 192 168 30 1/500 remote crypto	local crypto endpt : 192 168 10 1/500 remote crypto
andnt : 102 168 10 1/500	endpt : 102 168 30 1/500
path mtu 1500 insee overhead $78(44)$ modia mtu	noth mtu 1500 insee overhead $78(44)$ modie mtu
1500	1500
PMTU time remaining (sec): 0, DF policy: copy-df	PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets:	ICMP error validation: disabled, TFC packets:
disabled	disabled
current outbound spi: B7B5B38B	current outbound spi: F0C4239D
current inbound spi : F0C4239D	current inbound spi : B7B5B38B
inbound esp sas:	inbound esp sas:
spi: 0xF0C4239D (4039386013)	spi: 0xB7B5B38B (3082138507)
SA State: active	SA State: active
transform: esp-aes-256 esp-sha-256-hmac no	transform: esp-aes-256 esp-sha-256-hmac no
compression	compression
in use settings $-\{I, 2I, Tunnel, IKEy2, VTI\}$	in use settings $-\{1, 2\}$ Tunnel [KEy2 VTI]
alot 0 conn id 266 counts mone with counts mone	alot 0 conn idi 160 crunto moni viti crunto mon
sion 0, confined 200, crypto-map: $_vu$ -crypto-map-	siot: 0, conn_1d: 100, crypto-map: \vu -crypto-map-
sa timing: remaining key lifetime (kB/sec):	sa timing: remaining key lifetime (kB/sec):
(4285389/3722)	(3962829/3626)
IV size: 16 bytes	IV size: 16 bytes
replay detection support: Y	replay detection support: Y
Anti replay bitmap:	Anti replay bitmap:
0xFFFFFFFF 0xFFFFFFF	0xFFFFFFFF 0xFFFFFFF
outbound esp sas:	outbound esp sas:
spi: 0xB7B5B38B (3082138507)	spi: 0xF0C4239D (4039386013)
SA State: active	SA State: active
transform: esp-aes-256 esp-sha-256-hmac no	transform: esp-aes-256 esp-sha-256-hmac no
compression	compression
in use settings ={L2L. Tunnel. IKEv2. VTI. }	in use settings ={L2L. Tunnel. IKEv2. VTI. }
slot: 0, conn id: 266, crypto-map: vti-crypto-map-	slot: 0, conn id: 160, crypto-map. vti-crypto-map-
Tunnel1-0-1	Tunnel1-0-1
sa timing, remaining key lifetime (kR/sec).	sa timing, remaining key lifetime (kR/sec).
(A1A71A9/3722)	(A101069/3626)
$\frac{1}{1} \frac{1}{1} \frac{1}$	IV size: 16 bytes
ranlay detection support: V	replay detection support: V
Anti ronlow hitmon:	Anti ronlay hitman:
And replay blunap.	And replay billing. $0.0000000000000000000000000000000000$

Step 2. Navigate to the CLI of each FTD via console or SSH in order to verify the BGP status using the commands **show bgp neighbors** and **show route bgp**.

ftdv742# show bgp neighbors	ftdv742# show bgp neighbors
BGP neighbor is 169.254.10.2, vrf single_vf, remote	BGP neighbor is 169.254.10.1, vrf single_vf, remote
AS 65510, external link	AS 65511, external link
BGP version 4, remote router ID 192.168.50.1	BGP version 4, remote router ID 192.168.70.1
BGP state = Established, up for 1d20h	BGP state = Established, up for 1d20h
Last read 00:00:25, last write 00:00:45, hold time is	Last read 00:00:11, last write 00:00:52, hold time is
180, keepalive interval is 60 seconds	180, keepalive interval is 60 seconds
Neighbor sessions:	Neighbor sessions:
1 active, is not multisession capable (disabled)	1 active, is not multisession capable (disabled)
Neighbor capabilities:	Neighbor capabilities:
Route refresh: advertised and received(new)	Route refresh: advertised and received(new)
Four-octets ASN Capability: advertised and received	Four-octets ASN Capability: advertised and received
Address family IPv4 Unicast: advertised and received	Address family IPv4 Unicast: advertised and received
Multisession Capability:	Multisession Capability:
Message statistics:	Message statistics:
InQ depth is 0	InQ depth is 0
OutQ depth is 0	OutQ depth is 0
Sent Rcvd	Sent Rcvd
Opens: 1 1	Opens: 1 1
Notifications: 0 0	Notifications: 0 0
Updates: 2 2	Updates: 2 2
Keepalives: 2423 2427	Keepalives: 2424 2421
Route Refresh: 0 0	Route Refresh: 0 0
Total: 2426 2430	Total: 2427 2424
Default minimum time between advertisement runs is	Default minimum time between advertisement runs is
30 seconds	30 seconds
For address family: IPv4 Unicast	For address family: IPv4 Unicast
Session: 169.254.10.2	Session: 169.254.10.1
BGP table version 3, neighbor version 3/0	BGP table version 9, neighbor version 9/0
Output queue size : 0	Output queue size : 0
Index 1	Index 4
1 update-group member	4 update-group member
Sent Rcvd	Sent Rcvd
Prefix activity:	Prefix activity:
Prefixes Current: 1 1 (Consumes 80 bytes)	Prefixes Current: 1 1 (Consumes 80 bytes)
Prefixes Total: 1 1	Prefixes Total: 1 1
Implicit Withdraw: 0 0	Implicit Withdraw: 0 0
Explicit Withdraw: 0 0	Explicit Withdraw: 0 0
Used as bestpath: n/a 1	Used as bestpath: n/a 1
Used as multipath: n/a 0	Used as multipath: n/a 0
Outbound Inbound	Outbound Inbound
Local Policy Denied Prefixes:	Local Policy Denied Prefixes:
Bestpath from this peer: 1 n/a	Bestpath from this peer: 1 n/a
Total: 1 0	Total: 1 0
Number of NLRIs in the update sent: max 1, min 0	Number of NLRIs in the update sent: max 1, min 0
Address tracking is enabled, the RIB does have a	Address tracking is enabled, the RIB does have a
route to 169.254.10.2	route to 169.254.10.1
Connections established 1; dropped 0	Connections established 4; dropped 3
Last reset never	Last reset 1d21h, due to Interface flap of session 1

Transport(tcp) path-mtu-discovery is disabled Graceful-Restart is disabled	Transport(tcp) path-mtu-discovery is disabled Graceful-Restart is disabled
ftdv742# show route bgp Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per- user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF, BI - BGP InterVRF Gateway of last resort is 192.168.30.3 to network 0.0.0. B 192.168.50.0 255.255.255.0 [20/0] via 169.254.10.2, 1d20h	ftdv742# show route bgp Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per- user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF, BI - BGP InterVRF Gateway of last resort is 192.168.10.3 to network 0.0.0 B 192.168.70.0 255.255.255.0 [20/0] via 169.254.10.1, 1d20h

Step 3. Site1 Client and Site2 Client ping each other successfully.

Site1 Client:

Site1_Client#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/56/90 ms

Site2 Client:

Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

You can use those debug commands in order to troubleshoot the VPN section.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

You can use those debug commands in order to troubleshoot the BGP section.

```
ftdv742# debug ip bgp ?
```

```
BGP neighbor address
A.B.C.D
all All address families
events BGP events
import BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4 Address family
ipv6 Address family
keepalives BGP keepalives
        BGP Outbound information
BGP dynamic ---
out
range
             BGP dynamic range
rib-filter Next hop route watch filter events
updates BGP updates
         Address family
Address family
VRF scope
vpnv4
vpnv6
vrf
<cr>
```