# FortiGate Configuration (Mini DC Project)



### Job Requirements

Customer have 1 Dell server, 1 Cisco Catalyst Switch, 1 FortiGate 200F Firewall. Customer want to use Secure LAN network for Internet Access and also want to public their private web-Server.

### Service Component

- 1. Management Configuration
- 2. Interface & Basic Configuration
- 3. LACP
- 4. NAT Policy
- 5. Port Forwarding
- 6. Logging
- 7. Service Testing

### IP Address List

No	Zone Name	IP Address	Gateway	Remark
1	WAN	203.99.88.100/24	203.99.88.2	
2	Mgmt	192.168.1.99/24		
3	LACP			Port 3-4
4	Service	172.16.0.1/24	172.16.0.1	VLAN
5	Web-Server	172.16.0.10/24	172.16.0.1	



### 1. Initial Configuration

- > Connect to "MGMT" interface
- Set IP Address "192.168.1.100/24 " on management PC





#### Manual Configuration [via Console]

FortiGate-VM64-KVM # config system interface FortiGate-VM64-KVM (interface) # edit port1 FortiGate-VM64-KVM (port1) # set mode static FortiGate-VM64-KVM (port1) # set ip 192.168.1.99/24 FortiGate-VM64-KVM (port1) # set allowaccess https http ping ssh FortiGate-VM64-KVM (port1) # end FortiGate-VM64-KVM #

#### 2. Login to "FortiGate"

- ▶ browse <u>https://192.168.1.99</u>
- Username " admin" Password "no password"



#### 3. Configure Interface

$\leftrightarrow$ $\rightarrow$ G	2 192.168.1.99/ng/system/dashboard/1			☆ ♡ ④ ≦ =
🕞 FW-01 -	Ē			>_ 😧 • 🗘 🔁 • 👤 admin •
🙆 Dashboard 🗸 🗸	+ Add Widget			
Status			Sec. 184. area	
Security	System Information :-	Licenses 🕑 🕴 🚦	Virtual Machine	FortiGate Cloud
Network	Hostname FW-01	FortiCare Support	▲ FGVMEV License	Status O Not Supported
Users & Devices	Serial Number FGVMEVVG5DS-GY4A	Firmware & General Updates	Allocated vCPUs 1/1	
Signalling	Firmware v7.0.0 build0066 (GA)	O IPS	100%	
+	Mode NAT		Allocated RAM 997 MiB / 2 GiB	
FortiView Sources	System Time 2024/05/18 11:45:19	Andvirds	49%	
FortiView Destinations	Uptime 00:00:04:38	Web Filtering		
FortiView Applications	WAN IP Unknown	FortiToken 0/0	Auto Scaling 🖸 Disabled	
FortiView Web Sites		Unable to connect to FortiGuard servers.		
FortiView Policies				
FortiView Sessions	Security Fabric	Administrators I-	CPU	1 minute - I -
A Network		1 Console 1 HTTP 0 FortiExplorer	100%	
Policy & Objects		admin super_admin	75%	
Security Profiles	0		50%	
묘 VPN >	(DD)			
Leser & Authentication	🕞 FW-01		25%	
🕸 System 🚺 🗴			0%	
☆ Security Fabric >			11:44:22 11:44:33 11:4	44:43 11:44:53 11:45:04
년 Log & Report >	▲ Security Fabric Connection is disabled.		Current u	usage 2%
	Momony		Cossions	4 minuta - 1-

$\leftarrow \rightarrow $ C	O   192.168.1.99/ng/interface/edit/port2	
🕞 FW-01		
🕰 Dashboard	> Edit Interface	
Network      Interfaces      DNS      Packet Capture      SD-WAN      Static Routes      Policy Routes      RIP      area	Name       2         Alias       2         Type       WAN         VRF ID ③       0         Role ④       0         Estimated bandwidth       0         O       ©         kbps Upstream         0       ©         Address	FortiGate FW-4 Status Up MAC addr 50:00:00; Speed Tes
OSPF BGP Routing Objects Multicast	Address Address Addressing mode IP/Netmask Secondary IP address	Execute Additiona
<ul> <li>Policy &amp; Objects</li> <li>Security Profiles</li> <li>VPN</li> <li>User &amp; Authentication</li> <li>System</li> <li>Security Fabric</li> <li>Log &amp; Report</li> </ul>	Administrative Access  Administrative Access  IPv4 HTTPS SSH SNMP FMG FMG-Access FTM RADIUS Accounting Receive LLDP Use VDOM Setting Enable Disable Transmit LLDP Use VDOM Setting Enable Disable Traffic Shaping	<ul> <li>API</li> <li>Refe</li> <li>Edit</li> <li>Docur</li> <li>Onli</li> <li>Vide</li> </ul>
F	v7.0.0 OK Cancel	

### Interface Ready For "WAN"

$\leftarrow$	ightarrow C	C	2	192.168.1.99/ng/in	terface				
	🕏 FW-01	•	≡						
€® ‡	Dashboard <b>Network</b>	> ~	•	🕄 FortiGate VM64					
	DNS	ជ							
	Packet Capture		+	Create New -	🖋 Edit 🛍 Delete 🕨	Integrate Interfa	ce	Search	
	SD-WAN			Name ≑	Type 🗢	Members 🗘		IP/Netmask 🗢	Administrative Access 🖨
	Static Routes			♣ 802.3ad Aggreg	gate 1				
	RIP			ffortilink	₿ 802.3ad Aggregate		Dedi	cated to FortiSwitch	PING Security Fabric Connection
	OSPF			🔚 Physical Interfa	ce 4				
	BGP Routing Objects Multicast			m port1	Physical Interface		192.	168.1.99/255.255.255.0	PING HTTPS SSH
2	Policy & Objects	>		m port3	Physical Interface		0.0.0	.0/0.0.0.0	
	Security Profiles	> 、		m port4	Physical Interface		0.0.0	0.0/0.0.0.0	
 ▲	VPN User & Authentication	` ``		🖮 WAN (port2)	Physical Interface		203.	99.88.100/255.255.255.0	PING
- ✿ ※	System Security Fabric Log & Report	<ol> <li>*</li> <li>*</li> <li>*</li> <li>*</li> </ol>							
	F#RTINET	v7.0.0	0	Security Rating Issue	25				

#### 4. Configure LAN interface



#### Configure "Aggregate Interface"

$\leftarrow \rightarrow $ C	(	🔿   192.168.1.99/ng/i	nterface/edit					
🗊 FW-01	•	=						
🙆 Dashboard		New Interface						
Network     Interfaces     DNS     Packet Capi     SD-WAN     Static Route     Policy Rout     RIP	es	Name Alias Type VRF ID <b>3</b> Interface members Role <b>3</b>	LACP B• 802.3ad Aggregate 0 m port3 x m port4 + LAN	×	2 Choose LACP Protocol LACP Memebers			
OSPF		Address	Address					
BGP Routing Ob Multicast	jects	Addressing mode IP/Netmask Create address obje	Addressing mode     Manual     DHCP     Auto-managed by FortilPAM       IP/Netmask     0.0.0.0/0.0.0.0					
<ul> <li>Policy &amp; Ob</li> <li>Security Pro</li> <li>VPN</li> </ul>	jects > ofiles >	Name Destination Secondary IP addre	ss 🔿	LACP address 0.0.0.0/0.0.0				
User & Auth	nentication >	Administrative Acce	ess					
Security Fal	rt >	IPv4 Receive LLDP <b>(</b> )	HTTPS SSH RADIUS Accounting Use VDOM Setting Er	PING SNMP Security Fab Connection Disable Disable	FMG-Access FTM Fic			
FØF	<b>RTINET</b> v7.0.0				OK Cancel			

### "Aggreate" interface ready

$\leftarrow$ -	← → C 🛇 🖄 192.168.1.99/ng/interface							
🕞 FV	V-01	-	≡					
Øð Das	shboard <b>twork</b> erfaces	> ✓	633	FortiGate VM64				
DN	IS				2 4 6 8 10 1	2 14 16 18 20 22	24	
Pac	cket Capture		+ (	Create New -	🖋 Edit 🗎 🕮 Delete 🕨	Integrate Interfa	ce Search	
SD-	-WAN			Name 🗢	Type 🗢	Members 🗢	IP/Netmask 🗢	Administrative Access 🖨
Stat	tic Routes		<b>= *</b>	<ul> <li>802.3ad Aggreg</li> </ul>	gate 2			
Poli RIP	cy Routes	8	• fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection	
OSI BGI	iPF iP		÷	<ul> <li>LACP</li> </ul>	₿• 802.3ad Aggregate	m port3 port4	0.0.0.0/0.0.0.0	PING
Rou	uting Objects			Physical Interfa	ce 🤰			
Mu 🖻 Poli	ılticast licy & Objects curity Profiles	icast y & Objects > rity Profiles >		m port1	🖩 Physical Interface		192.168.1.99/255.255.255.0	PING HTTPS SSH
	N	>		WAN (port2)	Physical Interface		203.99.88.100/255.255.255.0	PING
Luse Sys Sec ⊡Log	er & Authentication stem curity Fabric g & Report	> 1 > > >						
	FCRTINET	v7.0.0	0 5	ecurity Rating Issue	es			

### 5. Create VLAN for Service Network

$\leftarrow$	$\rightarrow$ G	🔿   192.168.1.99/ng/ir	8 192.168.1.99/ng/interface						
6	≩ FW-01 <del>-</del>	=							
€® ‡	Dashboard > Network ✓ Interfaces	EFortiGate VM64	1-KVM 1 3 5 7 9 1	1 13 15 17 19 21 2 M M M M M M M	23				
	DNS Packet Capture	+ Create New -	2 4 6 8 10 1	2 14 16 18 20 22 2	ce Search				
	sd-wan 2	Interface	Type 🗢	Members 🖨	IP/Netmask 🗢	Administrative Access 🖨			
	Static Routes	Zone	gate 2						
	Policy Routes RIP	₿• fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection			
	OSPF BGP	B LACP	802.3ad Aggregate	m port3	0.0.0.0/0.0.0.0	PING			
	Routing Objects	😑 🔚 Physical Interfa	ace 2						
₽ ₽	Multicast       Policy & Objects       Security Profiles	im port1	Physical Interface		192.168.1.99/255.255.255.0	PING HTTPS SSH			
묘	VPN >	酬 WAN (port2)	Physical Interface		203.99.88.100/255.255.255.0	PING			
• <b>*</b> * •	User & Authentication > System 1 > Security Fabric > Log & Report >								
		0 Security Rating Issue	es						

$\leftarrow$ $\rightarrow$ C	$\bigcirc 8$	192.168.1.99/ng/interfac	e/edit				
🕞 FW-01 🔹 🗸	≡						
Dashboard     >	New Interface	3					
	Name	Service					
Interfaces 🏠	Alias			Choose Interface Type			
DNS	Туре	DE VLAN ✓					
Packet Capture	Interface			Choose Interface			
SD-WAN	VLAN ID	10	0				
Static Routes	VRF ID 🚯	0	0				
Policy Routes	Role 🕄	LAN	-				
RIP	A ddaeaa			Set LAN IP address			
OSPF	Address						
BGP	Addressing mode Matural DHCP Auto-mapaged by FortiliPAM						
Routing Objects	IP/Netmask		172.16.0.1/24				
Multicast	Create addre	ess object matching subhet 🗨					
Policy & Objects >	Destination		172 16 0 1/24				
Security Profiles	Secondary II	ndary IP address					
₽ VPN >	Secondary II	address					
User & Authentication >	Administrative Access						
💠 System 🚺 🕨	ID: 4	HTTPS	PING	FMG-Access			
☆ Security Fabric >	IPV4	SSH	SNMP	FTM			
Log & Report >		RADIUS Accounting	Security Fabric	Enable DHCP	server mode		
	C DHCP S	erver		Set DHCP range			
	DHCP status	🚯 Enabled 🔮 Disa	bled	Set Drice range			
	Address rang	ge 172.16.0.10-172.16.0	.254				
		C					
	Netmask	255.255.255.0					
	Default gate	way Same as Interface IP	Specify				
<b>F©RTINET</b> v7.0.0				O	K Cancel		

### Service VLAN Ready

$\leftarrow \rightarrow C$	0   1	92.168.1.99/ng/interface				☆
🕞 FW-01	• <b>=</b>					>_ 6
<ul> <li>Dashboard</li> <li>Network</li> </ul>	> ~	FortiGate VM64-KVM	<b>1 3</b> 5 7 9 11 13 15 17 19	21 23 m m		
Interfaces	☆	111	<b>2 4</b> 6 8 10 12 14 16 18 20	22 24		
DNS						
Packet Capture	+ (	Create New 🔻 🖋 Edit	🖻 Delete 🕨 Integrate Int	erface Search		Q
SD-WAN		Name 🗢	Type 🗢	Members ≑	IP/Netmask 🗘	Administrative Access 🗘
Static Routes		802.3ad Aggregate 3				
Policy Routes		tortilink	802 3ad Aggregate		Dedicated to FortiSwitch	PING
RIP			a corroad (BB) cBatc		Bealeated to Forthorntan	Security Fabric Connection
ospf Bgp		₽ LACP	₽ 802.3ad Aggregate	m port3	0.0.0.0/0.0.0.0	PING
Routing Objects		Service	왜 VLAN		172.16.0.1/255.255.255.0	PING
Multicast		Physical Interface 2				
<ul> <li>Policy &amp; Objects</li> <li>Security Profiles</li> <li>VPN</li> </ul>	> > >	m port1	🖷 Physical Interface		192.168.1.99/255.255.255.0	PING HTTPS SSH
User & Authentication	>	酬 WAN (port2)	Physical Interface		203.99.88.100/255.255.255.0	PING
<ul> <li>System</li> <li>Security Fabric</li> <li>Log &amp; Report</li> </ul>	> > >					
FCRTINET	v700 0 Se	ecurity Rating Issues				(

#### 6. Configure Static Route Go to Network>Static Routes>Create

$\leftarrow$	$\rightarrow$ G	$\bigcirc$ $\bigotimes$	192.168.1.99/ng/routing/static		
	穿 FW-01	- =			
æ	Dashboard	2 > +	Create New 🖋 Edit 🖬 Clone	🛍 Delete Search	
<b></b>	Network	✓ ~	Destination 🚔	Gateway IP ≜	Interfa
	Interfaces			Gatewayin	
	DNS				
	Packet Capture				
	SD-WAN				
	Static Routes	☆			
	Policy Routes				
	RIP				
	OSPF				
	BGP				
	Routing Objects				
	Multicast				No rest
-	Policy & Objects	>			
•	Security Profiles	>			
묘	VPN	>			
-	User & Authentication	>			
•	System	1 >			
*	Security Fabric	>			
1.11	Log & Report	>			
	EBTIDET				
		v7.0.0			



### Static Route Ready

$\leftarrow \  \  \rightarrow \  \  \mathbf{C}$	08	3 192.168.1.99/ng/routing/static			5	
🕞 FW-01	- =	=				
🕶 Dashboard	> -	+Create New 🖋 Edit 🗖 Clone	Delete Search		Q	
Network	~	Destination 🗢	Gateway IP ≑	Status ≑		
Interfaces			,			
DNS			202.02.02.0		Construct	
Packet Capture	0.0	0.0.0/0	203.99.88.2	WAN (port2)	S Enabled	
SD-WAN						
Static Routes	☆					
Policy Routes						
RIP						
OSPF						
BGP						
Routing Objects						
Multicast						
💄 Policy & Objects	>					
Security Profiles	>					
II VPN	>					
User & Authentication	>					
🏟 System	1 >					
🔆 Security Fabric	>					
Log & Report	>					
FURTIDET						

### Firewall Policy For "LAN-To-WAN"

$\leftarrow$	$\rightarrow$ G	0	🛇 🗞 192.168.1.99/ng/firewall/policy/policy/standard						
Ē	FW-01	•	≡						
æ	Dashboard		+ Create New / Edit Delete Q Policy Lookup Search						
\$	Network	<i></i> ,	Name	Source	Destination	Schedule	Service	Action	NAT
2	Policy & Objects	~							
	Firewall Policy	) ☆	Implicit Denv	ान all	الد 🗐				
	IPv4 DoS Policy		Implicit Delly				M ALL	<b>U</b> LINI	
	Addresses								
	Internet Service Database								
	Services								
	Schedules								
	Virtual IPs								
	IP Pools								
	Protocol Options								
	Traffic Shaping								
≙	Security Profiles	>							
묘	VPN	>							
-	User & Authentication	>							
\$	System	1 >							
*	Security Fabric	>							
ы	Log & Report	>							
	F	v7.0.0	0 Security Rating	Issues					



$\leftarrow$	$\rightarrow$ C	0	192.168.1.99/ng/	/firewall/policy/policy/sta	andard?showInList	{"q_origin_key":1	}			z
	🕏 FW-01	-	=							
æ	Dashboard		+ Create New	🖋 Edit 🗎 🖻 Delete	Q Policy Loo	kup Search				Q
<b>.</b>	Network		Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
4	Policy & Objects	~		M(A N) (====+2)						,
	Firewall Policy	☆	□ 📲 service → 📠							
	IPv4 DoS Policy		LAN-IO-WAN	Service address	i all	<b>C</b> always	LU ALL	ACCEPT	Enabled	SSL certificate-inspection
	Addresses		🖃 Implicit 🕁				_			
	Internet Service		Implicit Deny	😐 all	🗊 all	🐻 always	🖸 ALL	Ø DENY		
	Database									
	Services				·					
	Schedules				Λ.					
	Virtual IPs				LA	AN TO WAN	l Policy R	eadv		
	IP Pools									
	Protocol Options									
	Traffic Shaping									
•	Security Profiles									
묘	VPN									
-	User & Authentication									
\$	System									
*	Security Fabric									
[.11]	Log & Report									
	FURTIDET	v7.0.0	0 Security Rating Is	sues						

### 7. Create "Virtual IP"

$\leftarrow$	ightarrow $ ightarrow$ $ m G$	C	) 👌 192.168.1.99/ng/firewall/virtual-ip		
	FW-01	-	=		
æ	Dashboard 2	) >	+Create New - 🖉 Edit 「	Clone 🛍 Delete Search	
÷	Network	>	Name 🗢	Details 🗢	Interfaces 🗢
_ ₽	Policy & Objects	~			
	Firewall Policy				
	IPv4 DoS Policy				
	Addresses				
	Internet Service Database				
	Services				
	Schedules 1				
	Virtual IPs	☆			
	IP Pools				
	Protocol Options				No results
	Traffic Shaping				
	Security Profiles	>			
묘	VPN	>			
-	User & Authentication	>			
\$	System 🗧	>			
*	Security Fabric	>			
<u>Lui</u>	Log & Report	>			
	FERTIDET	7.0.0			

### Binding with [external public ip and port] to [internal private ip and port]

$\leftarrow \rightarrow \mathbf{G}$	🛇 👌 192.168.1.99/ng/firewall/virtual-ip/edit	
🕞 FW-01		
Dashboard	> New Virtual IP	
Network     Policy & Objects     Firewall Policy     IPv4 DoS Policy     Addresses	VIP type     IPv4       Name     Public-Web       Comments     Write a comment       Color     Change	Fo Ad
Internet Service Database Services Schedules Virtual IPs	Network       Interface ①     2       Type     Static NAT FQDN       External IP address/range     203.99.88.100       Mapped IP address/range     172.16.0.10	0
Protocol Options Traffic Shaping	Optional Filters     Set Internal Server IP	
<ul> <li>Security Profiles</li> <li>VPN</li> <li>User &amp; Authentication</li> <li>System</li> </ul>	Port Forwarding      Protocol      External service port     Map to port	
옷 Security Fabric 迪 Log & Report	> (3) OK Cancel	
FERTIDET	v7.0.0	

#### $\leftarrow \rightarrow$ C 🔿 👌 192.168.1.99/ng/firewall/policy/policy/standard/edit 🕞 FW-01 New Policy Network Policy & Objects Name 🚯 PF-Web Set Incomming & Outgoing Interface --MAN (port2) Incoming Interface IPv4 DoS Policy Outgoing Interface Service \*-Addresses Source 😑 all \* Source "All" Destination 🖀 Public-Web × Destination For "Virtual IP" G always • Schedule ALL\_ICMP HTTP HTTPS ×××× Service ACCEPT Ø DENY Action **Allow Services** Inspection Mode Flow-based Proxy-based 🚨 User & Authen Firewall / Network Options NAT O IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool 네 Log & Report Preserve Source Port 🕥 Protocol Options PROT default - / Security Profiles 0 AntiVirus Web Filter DNS Filter • Application Control 👁 0 IPS File Filter SSL Inspection ss. no-inspection - / Logging Options Log Allowed Traffic Security Events All Sessions Generate Logs when Session Starts 🕥 Capture Packets Comments Write a comment... /// 0/1023 Enable this notice Cancel ок

#### Create Port Forwarding Firewall Policy For "Public

#### Policy Ready For "WAN-To-LAN" DNAT

÷	$\rightarrow$ C		0   192.16	2 👌 192.168.1.99/ng/firewall/policy/policy/standard									♥ ④ ੬ ≡			
G	₿ FW-01	-	=	≻ <b>0-</b> û									4 <b>2 -</b> 😢 admin <del>-</del>			
Ð	Dashboard	>	+ Create New	F Create New										face Pair View By Sequence		
ф -	Network	>	Name	From	То	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes		
-	Policy & Objects	×	PF-Web	MAN (port2)	Service	💷 all	Public-Web	🖸 always	ALL_ICMP	✓ ACCEPT	Enabled	ssu no-inspection	🗢 All	0 B		
	IPv4 DoS Policy	ਮ							HTTP HTTPS							
	Addresses		LAN-To-WAN	Dill Service	MAN (port2)	Service address	😑 all	🐻 always	🕢 ALL	✓ ACCEPT	Enabled	ss. no-inspection	🗢 All	0 B		
	Internet Service Database		Implicit Deny	🗆 any	🗆 any	😐 all	😑 all	o always	😨 ALL	Ø DENY			Enabled	0 B		
	Schedules															
	IP Pools															
	Protocol Options															
	Traffic Shaping															
≙	Security Profiles	>														
묘	VPN	>														
-	User & Authentication	>														
\$	System (	1 >														
*	Security Fabric	>														
ш	Log & Report	>														

#### 8. LACP configuration on cisco switch

**Port-Channel Configuration** 

Switch(config)#hostname CS CS(config)#int range eth 0/0-1 CS(config-if-range)#desc /// AGG-TO-FGT /// CS(config-if-range)#channel-group 10 mode active exit

#### Trunk Configuration on "Agg Interface"

CS(config)#int port-channel 10 CS(config-if)#description /// AGG-TO-FGT /// CS(config-if)#switchport trunk encapsulation dot1q CS(config-if)#switchport mode trunk CS(config-if)#exit

#### Create Vlan [Service vlan 10]

CS(config)#vlan 10 CS(config-vlan)#name SERVICE CS(config-vlan)#exit CS(config)#

#### Create Access Vlan 10

CS(config)#int eth 0/2 CS(config-if)#no sh CS(config-if)#desc /// TO WEB-SERVER /// CS(config-if)#switchport mode access CS(config-if)#switchport access vlan 10 CS(config-if)#switchport nonegotiate CS(config-if)#exit CS(config)#

#### Check Etherchannel Status

CS#sh etherchannel summary Number of channel-groups in use: 1 Number of aggregators: 1

Group Port-channel Protocol Ports

10	Po10(SU)	LACP H	t0/0(P)	Et0/1(	(P)						
<u>Chec</u>	<u>ck Trunk Stat</u>	<u>us</u>									
CS#s	how int trunk										
Port Po10	Mode on	Encapsu 802.1c	ation S tru	tatus ınking	Nati	ve vlan 1					
Port Po10	Vlans allo 10	wed on trun	5								
Port Po10	Vlans allo 10	Vlans allowed and active in management domain 10									
Port Po10	Vlans in s 10	panning tree	forward	ing state	e and n	ot prun	ned				

## Service Testing

### Ping Test From "LAN" to "8.8.8.8"

E1 - OSPF external type 1, E2 - OSPF external type 2 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 rout o - ODR, P - periodic downloaded static route, H - NHRP, 1 - LISP + - replicated route, % - next hop override	e
Gateway of last resort is 172.16.0.1 to network 0.0.0.0	
<pre>S* 0.0.0.0/0 [1/0] via 172.16.0.1 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks C</pre>	
L 172.16.0.10/32 is directly connected, Ethernet0/0	
WEB# WEB#ping 8 8 8 8	
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds: !!. Success rate is 40 percent (2/5), round-trip min/avg/max = 69/80/92 ms	
WEB#ping 8.8.8.8 Type escape sequence to abort. Sending 5. 100-byte ICMP Echos to 8.8.8.8. timeout is 2 seconds:	
Success rate is 100 percent (5/5), round-trip min/avg/max = 69////82 ms	

$\leftarrow \  \  \rightarrow \  \  \mathbf{C}$		🔿   192.168.1.99/ng/ld	og/view/traffic/f	orward				90%	♡ ③ ∱ ≡
FortiGate VM64-KVM	A FortiC	Gate-VM64-KVM						Q+ >_ []	@• 🗘 🛛 🕗 admin•
Dashboard	>	C 🛓 💿 Add Filter	r						🕞 🔹 🔲 Details
🔆 Security Fabric	>	Date/Time	0	Source	Device	Destination	Application Name	Desult	Policy ID
Network	> _	Date/ 1111c	0	170.14.0.10			Application Hame	- 500 D (00 1 D	Toncy ID
System	> <sup>2</sup>	2024/05/18 08:28:09		172.16.0.10	aa:bb:cc:00:30:00	8.8.8.8 (dns.google)		✓ 500 B / 384 B	LAN-Io-WAN (1)
Policy & Objects	> 2	2024/05/18 08:27:53		172.16.0.10	aa:bb:cc:00:30:00	🎫 8.8.8.8 (dns.google)		✓ 500 B / 384 B	LAN-To-WAN (1)
Security Profiles	> 2	2024/05/18 08:27:33		172.16.0.10	aa:bb:cc:00:30:00	8.8.8.8 (dns.google)		✓ 2.00 kB / 1.82 kB	LAN-To-WAN (1)
L VPN	> 2	2024/05/18 08:25:46		172.16.0.10	aa:bb:cc:00:30:00	8.8.8.8 (dns.google)		✓ 500 B / 480 B	LAN-To-WAN (1)
User & Authentication	> 2	2024/05/18 08:25:06		203.99.88.1		203.99.88.100		✓ 527 B/341 B	PF-Web (2)
🔟 Log & Report	~ 2	2024/05/18 08:25:03		203.99.88.1		203.99.88.100	$\backslash$	✓ 574 B / 396 B	PF-Web (2)
Forward Traffic	☆ 2	2024/05/18 08:16:03		203.99.88.1	$\backslash$	203.99.88.100	$\backslash$	✓ 260 B / 400 B	PF-Web (2)
Local Traffic	2	2024/05/18 08:16:03		203.99.88.1	Course ID	203.99.88.100		×	PF-Web (2)
Sniffer Traffic	2	2024/05/18 08:16:02		203.99.88.1	Source IP	203.99.88.100	Destination IP	✓ 260 B / 400 B	PF-Web (2)
Events	2	2024/05/18 08:16:02		203.99.88.1		203.99.88.100		×	PF-Web (2)
AntiVirus	2	2024/05/18 08:15:41		203.99.88.1		203.99.88.100		✓ 260 B / 320 B	PF-Web (2)
Web Filter	2	2024/05/18 08:15:41		203.99.88.1		203.99.88.100		×	PF-Web (2)
SSL	2	2024/05/18 08:15:41		203.99.88.1		203.99.88.100		✓ 260 B / 320 B	PF-Web (2)
DNS Query	2	2024/05/18 08:15:41		203.99.88.1		203.99.88.100		×	PF-Web (2)
File Filter	2	2024/05/18 08:15:41		203.99.88.1		203.99.88.100		✓ 260 B / 320 B	PF-Web (2)
Application Control	2	2024/05/18 08:15:41		203.99.88.1		203.99.88.100		~	PF-Web (2)
Intrusion Prevention	2	2024/05/18 08:15:34		203.99.88.1		203.99.88.100		✓ 260 B / 320 B	PF-Web (2)
Anomaly	2	2024/05/18 08:15:34		203.99.88.1		203.99.88.100		×	PF-Web (2)
Log Settings	2	2024/05/18 08:15:23		203.99.88.1		203.99.88.100		✓ 156 B / 240 B	PF-Web (2)
Threat Weight	2	2024/05/18 08:15:23		203.99.88.1		203.99.88.100		×	PF-Web (2)
	2	2024/05/18 08:15:22		203.99.88.1		203.99.88.100		✓ 156 B / 240 B	PF-Web (2)
									0% 22

#### Check Logging From "LAN-172.16.0.10" To "8.8.8.8"

#### Check Public Web Server Access From "Public"

#### Check Lan IP



### Browse to Public IP (WAN IP)

$\leftrightarrow \rightarrow X$ Q 203.99.88.100	(	. ⊜	பி	≡
🕣 Import bookmarks 👋 Getting Started 🤣 Roundcube Webmail 📴 IPSEC VPN and NAT-T 🏦 IOS Router to Pass a L. 🔮 Training Institute: Sche 👽 Zeus Cloud - Cloud Se 📓 Site-to-Site VPN betw 👌 The Complete Cisco I	N			$\gg$
				\$
adminSign in Cancel				
G Search with Google or enter address				
networkcloudl 192168.197.128 youtube 1721611.1 192168.101.132 10.10.1 cloudiabnetwo 1721611.21				

### Successfully Access to [Private Web-Server] From [Public]

$\leftarrow \rightarrow C$ $\bigcirc \& 203.99.88.100$	
Cisco Systems	
Accessing Cisco Unix "WEB"	
Show diagnostic log - display the diagnostic log. Monitor the router - HTML access to the command line interface at level <u>0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15</u>	
<u>Show tech-support</u> - display information commonly needed by tech support. <u>Extended Ping</u> - Send extended ping commands.	
<u>QoS Device Manager</u> - Configure and monitor QoS through the web interface.	
Help resources	
<ol> <li><u>CCO at www.cisco.com</u> - Cisco Connection Online, including the Technical Assistance Center (TAC).</li> <li><u>tac@cisco.com</u> - e-mail the TAC.</li> </ol>	
<ul> <li>3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.</li> <li>4. <u>cs-html@cisco.com</u> - e-mail the HTML interface development group.</li> </ul>	

Aung Zin Phyo Sr.Network Engineer

+95-9897842856