Palo Alto Feature Basic Configuration Guide On PAN-OS 7.1.0



By : L30

# Daftar Isi

1.	Config Penambahan Interface VM Palo Alto	3					
2.	Change Password Administrator	9					
3.	Konfigurasi Interface Management	9					
4.	Configure Hostname, Timezone, Banner Login, Domain etc						
5.	Configure DNS Server, Update Server, Proxy Object, NTP Server	10					
6.	Configure Administrator dan Password	11					
7.	Config Intrerface	12					
8.	Konfigurasi Zone	14					
9.	Allowed Access to Interface Firewall (Management Profile Interface)	15					
10.	Basic Configuration Policy	16					
11.	Basic Configure NAT	19					
a.	DNAT	19					
a. b.	DNAT	19 21					
a. b. 12.	DNAT SNAT Basic Konfigurasi Global Protect	19 21 23					
<b>a.</b> <b>b.</b> 12. 13.	DNAT SNAT Basic Konfigurasi Global Protect Basic Konfigurasi Split Tunneling	19 21 23 39					
<b>a.</b> <b>b.</b> 12. 13. 14.	DNAT SNAT Basic Konfigurasi Global Protect Basic Konfigurasi Split Tunneling Konfigurasi Palo Alto Join AD (Agentless)	19 21 23 39 40					
<b>a.</b> <b>b.</b> 12. 13. 14. 15.	DNAT SNAT Basic Konfigurasi Global Protect Basic Konfigurasi Split Tunneling Konfigurasi Palo Alto Join AD (Agentless) Reset Factory Default configurasi Palo Alto (setelah berhasil Login)	19 21 23 39 40 54					
<b>a.</b> <b>b.</b> 12. 13. 14. 15. 16.	DNAT SNAT Basic Konfigurasi Global Protect Basic Konfigurasi Split Tunneling Konfigurasi Palo Alto Join AD (Agentless) Reset Factory Default configurasi Palo Alto (setelah berhasil Login) Reset Factory default config dan reset password administrator	19 21 23 39 40 54 55					
<ul> <li>a.</li> <li>b.</li> <li>12.</li> <li>13.</li> <li>14.</li> <li>15.</li> <li>16.</li> <li>17.</li> </ul>	DNAT SNAT Basic Konfigurasi Global Protect Basic Konfigurasi Split Tunneling Konfigurasi Palo Alto Join AD (Agentless) Reset Factory Default configurasi Palo Alto (setelah berhasil Login) Reset Factory default config dan reset password administrator Ipsec VPN Site to Site (Static Route)	19 21 23 39 40 54 55 59					
<b>a.</b> <b>b.</b> 12. 13. 14. 15. 16. 17. 18.	DNAT SNAT Basic Konfigurasi Global Protect Basic Konfigurasi Split Tunneling Konfigurasi Palo Alto Join AD (Agentless) Reset Factory Default configurasi Palo Alto (setelah berhasil Login) Reset Factory default config dan reset password administrator Ipsec VPN Site to Site (Static Route) Failover Link Used PBF 2 ISP (Policy Based Forwarding)	19 21 23 39 40 54 55 59 69					
a. b. 12. 13. 14. 15. 16. 17. 18. 19.	DNAT         SNAT         Basic Konfigurasi Global Protect         Basic Konfigurasi Split Tunneling         Konfigurasi Palo Alto Join AD (Agentless)         Reset Factory Default configurasi Palo Alto (setelah berhasil Login)         Reset Factory default config dan reset password administrator         Ipsec VPN Site to Site (Static Route)         Failover Link Used PBF 2 ISP (Policy Based Forwarding)         ECMP Load Balancing	19 21 23 39 40 55 59 69 75					

# 1. Config Penambahan Interface VM Palo Alto

Setelah kita melakukan instalasi default Palo Alto Virtual, maka akan kita dapat lihat secara default palo alto virtual hanya memiliki dua virtual interface unterface, satu diperuntukkan untuk mgmt interface satu lagi digunakan untuk interface Network Palo Alto, namun dalam melakukan konfigurasi firewall kita sangat membutuhkan minimal 2 interface network (internal dan external) agar firewall tersebut dapat berjalan dengan baik, pertama lakukan shutdown pada palo alto virtual pada vm host anda, kamudian lakukan penambahan interface seperti contoh di bawah

Virtual Macł	hine Settings				>
Hardware	Options				
Device	ory essors Disk (SCSI) WD (IDE) rork Adapter rork Adapter 2 ay	Summary 4 GB 2 40 GB Auto detect Bridged (Automatic) Bridged (Automatic) 1 monitor		Device status Connected Connect at power on Network connection Bridged: Connected directly to the physical network Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network VMnet1 (Host-only) LAN segment: LAN Segments Advanced	
		Add	Remove		

Jika kita ingin menambahkan interface virtual ke dalam Palo alto virtual system kita dapat melakukanya dengan cara melakukan penambahan pada virtual machine setting Add  $\rightarrow$  Network Adapter Type : Custom  $\rightarrow$  Device Status : Checklist  $\rightarrow$  Finish

options			
Device	Summary	Device status	
Memory	4 GB	Connected	
Processors	2	Connect at power on	
Hard Disk (SCSI)	Add Hardware Wizard		×
Network Adapter	Network Adapter Type		ysical network
Network Adapter 2	What type of network adapter do	ction state	
<u> </u>	Network connection		ress
		uvsical network	with the host
	Replicate physical network conner	ction state	
		race	~
	O Host-only: A private network shared	with the host	$\sim$
	Custom: Specific virtual network		
	VMnet4	~	nts Advanced
	Device status		-
	Connect at power on		
	<	Cancel	

Maka kita selanjutnya kita akan melihat virtual interface yang baru saja kita tambahkan ke dalam palo alto system seperti contoh gambar di bawah

Virtual Machine Settings		×
Hardware Options		
Device Memory Processors Hard Disk (SCSI) CD/DVD (IDE) Network Adapter 2 Network Adapter 3 Display	Summary 4 GB 2 40 GB Auto detect Bridged (Automatic) 2 Bridged (Automatic) 3 Custom (VMnet2) 1 monitor 1 monitor Remove	Device status Connected Connect at power on Network connection Bridged: Connected directly to the physical network Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network VMnet2 (Host-only) LAN segment: LAN Segments Advanced
		OK Cancel Help

Setelah konfigurasi terlihat seperti gambar di atas, jangan lakukan start pada system palo alto virtual terlebih dhulu, karena secara default interface yang baru saja kita tambahkan memiliki type "e1000" sedangkan interface type yang compatible dengan palo alto system adalah "vmxnet3" maka dari itu ketika kita melakukan power on pada palo alto system tanpa melakukan perubahan pada interface type yang baru saja kita tambahkan akan menimbulkan error pada saat melakukan booting, untuk melakukan perubahan type virtual interface pada palo alto virtual lakukan seperti contoh di bawah ini

Masuk kedalam direktori Virtual Machine workstation pada direktori OS windows 10 Document  $\rightarrow$  Virtual Machine  $\rightarrow$  PALO <virtual machine workstation name>  $\rightarrow$  (edit with notepad) PALO.vmx

Lakukan perubahan kepada interface virtual yang baru saja kita tambahkan etehernet.2 kepada type vmxnet3 dengan mencontoh dari virtual interface sebelumnya ethernet.1

Exisiting

```
ethernet1.present = "TRUE"
ethernet1.virtualDev = "vmxnet3"
ethernet1.connectionType = "bridged"
ethernet1.startConnected = "TRUE"
ethernet1.addressType = "generated"
```

New

```
ethernet2.present = "TRUE"
ethernet2.vnet = "VMnet2"
ethernet2.connectionType = "custom"
ethernet2.virtualDev = "vmxnet3"
ethernet2.wakeOnPcktRcv = "FALSE"
ethernet2.addressType = "generated"
```

selanjutnya lakukan save perubahan kemudian lakuan power On virtual machine palo alto virtual system, sehingga muncul halaman loggon admin pada console nterface virtual machine,

secara default login administrator palo alto firewal virtual adalah user : admin pass : admin

setelah login masuk ke dalam menu configurasi untuk melihat konfigurasi awal/default palo alto firewall virtual seperti gambar di bawah

```
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# show deviceconfig
deviceconfig {
  system {
    ip-address 192.168.1.1;
    netmask 255.255.255.0;
    update-server updates.paloaltonetworks.com;
    update-schedule {
      threats {
        recurring {
          weekly {
            day-of-week wednesday;
            at 01:02;
            action download-only;
    timezone Asia/Jakarta;
    service {
      disable-telnet yes;
      disable-http yes;
    hostname PA-VM;
  setting {
    config {
      rematch yes;
    management {
      hostname-type-in-syslog FQDN;
[edit]
admin@PA-VM#
```

Login melalui browser untuk mengakses web configuration menggunakan IP address management palo alto system yaitu **192.168.1.1** menggunakan protocol https



Login menggunakan user dan password default, untuk masuk ke dalam halaman configurasi administrator palo alto firewall seperti gambar di bawah ini

$\leftrightarrow \rightarrow \mathbf{C}$ A Tidak amar	h   bttps://192.168.1.1/#dashboard::		☆ 🗷 🦉 🗄
paloalto	Dashboard ACC Mo	nitor Policies Objects Network Device	🍰 Commit 💣 🖻 Save 🔍 Search
General Information		S 🗙 Logged In Admins S 🗙 Config Lo	gs 🖸 🗙
Device Name	PA-VM	Admin Form Client Consist Address No.data.as	ailable
MGT IP Address	192.168.1.1	weicome	0
MGT Netmask	255.255.255.0	(f)	e x
MGT Default Gateway		~	
MGT IPv6 Address	unknown	Welcome to PAN-OS 7 11	
MGT IPv6 Link Local Address	fe80::20c:29ff:fea1:c005/64		Last 60 minutes) G X
MGT IPv6 Default Gateway		This release includes many new features, including this message of the day. Some highlights of this release include:	
MGT MAC Address	00:0c:29:a1:c0:05		
Model Carial #	PA-VM	<ul> <li>SaaS Application Usage Report for visibility into sanctioned and unsanctioned SaaS applications running on your network.</li> <li>Sunnort for large-scale_distributed liser-ID danloyments</li> </ul>	
CRUID	E3060500EEEBAB1E	AutoFocus threat intelligence integration with PAN-OS logs.	
UUTD	564D5E18-DBC0-CA27-E20D-2E136DA1C005	<ul> <li>Unified log view showing all traffic and threat-related logs on a single page.</li> </ul>	
VM License	none	<ul> <li>WildFire five-minute updates for detecting and blocking zero-day malware and exploits within minutes of discovery.</li> <li>External Deterministic (formatic Deterministic Plank Link) and added to support UDL and autom deterministic.</li> </ul>	
VM Mode	VMWare ESX	<ul> <li>External Dynamic Dists (romeny Dynamic Dick Dist) extended to support Drcs and custom domains.</li> <li>Support for the VM-Series firewall in Microsoft Azure.</li> </ul>	
Software Version	7.1.0	<ul> <li>Support for scaling the VM-Series firewall behind AWS Elastic Load Balancing (ELB).</li> </ul>	
GlobalProtect Agent	0.0.0	<ul> <li>Simplified deployment of two-factor authentication on GlobalProtect.</li> </ul>	
Application Version	564-3168	For a complete description of the new features and instructions on how to use them, refer to the PAN-OS 7.1 New Features Guide.	
URL Filtering Version	0000.00.000	To ensure that you can take advantage of all of the new features, you must upgrade the Content Release version. Refer to the PAN-	
Time	Sun Mar 26 21:32:48 2017	OS 7.1 Release Notes for the content version required.	
Uptime	0 days, 0:04:34		
System Resources		Do not snow again	
Management CPU	20%		
Data Plane CPU	3%	Close	
Session Count	0 / 1248		

### 2. Change Password Administrator

Hal yang paling utama yang harus dilakukan pertama yaitu merubah password default administrator palo alto firewall, kita dapat merubah password default administrator melalui menu **Device**  $\rightarrow$  **Administrators**, klik user admin yang akan diubah passwordnya, masukkan password lama dan password baru kemudian klik OK dan commit configurasi, contohnya seperti gambar di bwah

paloalto		Dashboard	ACC I	Monitor Poli	cies Object	ts Network	Device					
🖓 Setup 🔺	. 🔍											
Client Certificate Public Key												_
Config Audit		Name	Role	Authentication	Password Profile	Authentication	Authentication	Profile	Locked User			
Password Profiles				Profile		(Web)	(SSH)					
8 Administrators												
Admin Roles												
Authentication Profile												
Authentication Sequence												
VM Information Sources					Administre	atore			6	5		
Certificate Management					Administre	1013				4		
Certificates						Name	admin					
🔁 Certificate Profile						Old Password	1					
CCSP Responder						New Paceword	<u> </u>					
SSL/TLS Service Profile						New Password	•					
🔄 🕅 SCEP					Co	nfirm New Password	•					
Response Pages							Use Public Key	Authentication (SSH	)			
Log Settings												
Server Profiles								ОК	Cancel			
Similar Currier												
Email												
Netflow												
RADIUS												
TACACS+												
🐴 LDAP												
🐴 Kerberos												
V 🔝 Local User Database												
S Users												
S User Groups												
Scheduled Log Export												

### 3. Konfigurasi Interface Management

Lakukan perubahan konfigurasi interface management sesusai dengan segmen network management address yang kalian miliki, untuk mengubah IP address management kita bisa melalui menu

Device $ ightarrow$ Setup $ ightarrow$ Ma	anagement $ ightarrow$ Management	: Interface Setting $ ightarrow$
---	-----------------------------------	----------------------------------

Management Interface Set	tings		0
ІР Туре	Static O DHCP Client	Services	
IP Address	192.168.98.105	П НТТР	Permitted IP Addresses
Netmask	255.255.255.0	HTTP OCSP	
Default Gateway	192.168.98.1	HTTPS	
IPv6 Address/Prefix Length		Telnet	
Default IPv6 Gateway		SSH SSH	
Speed	auto-negotiate 💌	Ping	
MTU	1500	SNMP	
		User-ID	
		User-ID Syslog Listener-SSL	
		User-ID Syslog Listener-UDP	
			+ Add Delete
			OK Cancel

Lakukan konfigurasi IP Management dan gateway serta remote access yang diperbolehkan kepada IP Management seperti HTTPS, SSH, PING

# 4. Configure Hostname, Timezone, Banner Login, Domain etc

Selanjutnya adalah kita akan melakukan perubahan timezone, banner,domain name dan hostname palo alto virtual system melalui menu Device → Management G → General setting → Edit

General Settings 0 agement Operations Services Content-ID Wi Hostname PA-VM-Galaxi Domain galaxidata.com Accept DHCP server provided Hostname eceive Timeout for Connecti Accept DHCP server provided Domain Send Timeout for Connection t Login Banner This is Private Environment, everything you will do we Retry Count for SSL S Force Admins to Acknowledge alaways monitor SSL/TLS S Force Admins to Acknowledge Login Banner IP T IP Add SSL/TLS Service Profile None V Netm -Time Zone Asia/Jakarta Default Gate -Automatically Acquire Locale en IPv6 Addı Certificate Expi Date 2017/03/27 -IPv6 Default Gate Serv Use Hypervisor Assigned MA Time 11:45:39 -Latitude Longitude Automatically Acquire Commit Lock Me Allow Do I Certificate Expiration Check Use Hypervisor Assigned MAC Addresses Authenti Cancel ок Idle Timeout (min) 60 Failed Attempts 0

Lakukan konfigurasi seperti contoh gambar di bwah

### 5. Configure DNS Server, Update Server, Proxy Object, NTP Server

Lakukan konfigurasi DNS, Update, NTP server melalui menu Device  $\rightarrow$  Setup  $\rightarrow$  Services  $\rightarrow$ 

Services	<u></u>
DNS	Servers
Primary DNS Server	8.8.8.8
Secondary DNS Server	
Update Server	updates.paloaltonetworks.com
Verify Update Server Identity	
Proxy Server	
Primary NTP Server Address	192.168.1.44
Primary NTP Server Authentication Type	None
Secondary NTP Server Address	

Konfigurasi Salah satu DNS pada palo alto appliance karena jika tidak maka palo alto tidak akan bisa melakukan resolve domain untuk melakukan update, palo alto menggunakan interface management untuk melakukan komunikasi kepada wildfire, maka pastikan konfigurasi interface management dan default routenya serta konfigurasi DNS sudah dilakukan dengan benar. Jika palo alto membutuhkan proxy server untuk mencapai domain update maka masukkan settingan konfigurasi proxy

# 6. Configure Administrator dan Password

.akukan penambahan user administrator melalui menu Device -> Administrators -> 🍄 Add							
Administrator	•						
Name	Ihutapea						
Authentication Profile	None						
	Use only client certificate authentication (Web)						
Password	•••••						
Confirm Password							
Administrator Type	<ul> <li>Use Public Key Authentication (SSH)</li> <li>Dynamic O Role Based</li> </ul>						
	Superuser 💌						
Password Profile	None						
	OK Cancel						

# 7. Config Intrerface

Pada tahap selanjutnya kita akan melakukan konfigurasi interface firewall Palo alto system, karena secara default setiap interface yang dimiliki oleh palo alto virtual masih dalam kondisi down / not configured, jadi jika kita akan melakukan konfigurasi interface network minimal requirement firewall yaitu internal dan external, konfigurasi interface dapat dilakukan melalui menu **Network**  $\rightarrow$  **Interfaces** 

Interfaces 20 Zones	Ethernet VLAN Lo	opback Tunnel										
Marcones 당동 VLANs 원들 Virtual Wires ④ Virtual Routers												
	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual- Wire	Security Zone	Features	Comment	
DHCP	ethernet1/1			1	none	none	Untagged	none	none			
DNS Proxy	ethernet1/2			m	none	none	Untagged	none	none			
Portals	ethernet1/3				none	none	Untagged	none	none			
Gateways	ethernet1/4				none	none	Untagged	none	none			
MDM	ethernet1/5				none	none	Untagged	none	none			
& QoS	ethernet1/6				none	none	Untagged	none	none			
State LLDP	ethernet1/7				none	none	Untagged	none	none			
Network Profiles     Clabal Protect IPCoc Comta	ethernet1/8				none	none	Untagged	none	none			
IKE Gateways	ethernet1/9				none	none	Untagged	none	none			
Ⅲ IKE Gateways           Ⅲ ISE Crypto           Ⅲ IKE Crypto           № Monitor           № Monitor           № Zone Protection           № Zone Protection           № JUP Profile           № BFD Profile	*											

Sebelum di lakukan konfigurasi interface

Pertama klik interface yang akan dikonfigurasi contoh ethernet1/1 konfigurasi kedalam mode network yaitu Layer 3, assign interface tersebut kepada virtual router default untuk security zone berikan nilai None sementara karena selanjutnya kita akan membuat zone profile terlebih dahulu, hasil confi interface dapat dilihat pada gambar di bawah

paloalto	Dashboard AC	C Monito	r Policies	Obje	ects Network	Device	🍰 Commit 💰 🗟 Save	q, s
Interfaces Zones VLANs Dirtual Wires Virtual Routers	Ethernet VLAN Lo	opback Tunnel						
	Interface	Interface Type	Management	Link	IP Address	Virtual F	outer Tag VLAN / Virtual- security Zone Features Comment	
DHCP	ethernet1/1		Profile	State	none	none	Ethernet Interface	อ
DNS Proxy	ethernet1/2				none	none	Interface Name ethernet1/1	
V 😨 GlobalProtect	ethernet1/3			122	none	none	Comment	1
Gateways	ethernet1/4				none	none	Interface Type Layer3	í.
MDM Device Black List	ethernet1/5			1771	none	none	Netflow Profile None	1 I I
& QoS	ethernet1/6				none	none	Config IPv4 IPv6 Advanced	
CLDP	ethernet1/7			100	none	none		11.
Network Profiles     GlobalProtect IPSec Counts	ethernet1/8				none	none	Assign Interlace To	
H IKE Gateways	ethernet1/9				none	none	Virtual Router default	
A IPSec Crypto							Security Zone None	
A IKE Crypto								
IPE Crypto     Monitor     Toriantor     Toriantor     Zone Protection     Que Profile     Que Profile     QUE Profile							OK Canel	

Untuk memberikan interface tersebut IP address silahkan pilh subtab **IPv4** kemudian klik tombol add **New Address** kemudian isilah address IPV4 yang akan di assign kepada interface tersebut

E							0			
	Interface Name e	thernet1/1								
	Comment					Address				0
	Interface Type	ayer3				Name	External			
	Config IPvA		Advanced			Description	External Iface IP	address		
	Coning II V4					Туре	IP Netmask	▼ 192.168.99.152/	24 F	Resolve
	Type  Static  PPPoE  DHCP Client				Tags		notation (Ex. 192.16 can also enter an IP its prefix (Ex. 2001:d 2001:db8:123:11:/64	8.80.150 or 192.168.80.0) 6 address or an IPv6 addr b8:123:1::1 or )	(24). You ress with	
								l	OK Car	ncel
	🕂 Add 🖃 Delete	Move L	Jp 🕒 Move Dawn							
	IP address/netmask. Ex. 19	92.168.2.25	4/24							
							Cancel			

Klik OK. Selanjutnya lakukan konfigurasi management profile untuk interface tersebut seperti gambar di bawah, pilih **Advanced** pada option **Management profile** Klik drop down menu –> pilih **new management profile**, dan pilih allowed access kepada interface tersebut

	Mana	Interface Management Profile	(1) ity Zone	
	Profile	Name		
9	Ethernet	Permitted Services	Permitted IP Addresses	
н	Inter	Ping		
1		Telnet		
Т	Inte	SSH		
	Net	П НТТР		
Т	Config	□ HTTP OCSP		
1	Link	П нттря		
1	Linl	SNMP	<b>Y</b>	
1		Response Pages		
1	Other	User-ID		
1		User-ID Syslog Listener-SSL	V	
1		User-ID Syslog Listener-UDP	🕂 Add 📼 Delete	
			Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64	
1			OK Cancel	
1		Untagged Subinterface		
			OK Cancel	

lakukan commit untuk menyetujui perubahan konfigurasi, jika konfigurasi interface sukses maka status dari interface yang baru saja dikonfigurasi akan berubah menjadi berwarna hijau seperti gambar di bawah ini

paloalto	Dashboard	ACC	Monitor	Policies	Obje	cts Network D
Interfaces	Ethernet VLAN	Loopback	Tunnel			
🚧 Zones 😼 VLANs						
€∎ Virtual Wires ⊕ Virtual Routers ⊕ IPSec Tunnels	Interface	Interf	ace Type	Management Profile	Link State	IP Address
DHCP	ethernet1/1	Layer	3		m	External
DNS Proxy	ethernet1/2				m	none
GlobalProtect	ethernet1/3				m	none
Gateways	ethernet1/4				m	none
MDM 📢	ethernet1/5				and the	none

Selanjutnya kita akan melakukan konfigurasi profile Zone Firewall dan akan melakukan **assign zone** kepada interface external yang baru saja kita konfigurasi tersebut ,

# 8. Konfigurasi Zone

Konfigurasi zone dapat dilakukan melalui menu **Network → Zones** untuk menambahkan zone profile kita dapat mengklik tombol add dan lakukan konfigurasi untuk zone external

						User ID	
Name	Туре	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	Enabled	Included Networks	E
Z External	layer3	ethernet1/1				External	I
		Zone	News R is 1		User Identification AC	0	
			Name External		User Identification ACL		
			Service Prof	ile Zone for NSX	🔲 Include List 🔺		
			Type Layer3	~	External		
		Inter	rfaces 🔺				
		🔲 ethe	rnet1/1				
					🕂 Add 🗖 Delete		
					Users from these addresses/subnets will I	e identified.	
					Exclude List 🔺		
					Select an address or address gro	oup or type in your own	
		🕂 Add	- Delete		address. Ex: 192.168.1.20 or 192	1.168.1.0/24	
		7	to dia Desfie				
		Zone Pro	None None	•			
			Log Setting None		🕂 Add 🖃 Delete		
			Enable User	Identification	Users from these addresses/subnets will r	tot be identified.	
						OK	

Isikan name profile Zone, Interface yang akan di assign kepada zone tersebut dan List IP address yang berada pada zone tersebut (include list), jika usdah selesai klik OK dan lakukan Commit

# 9. Allowed Access to Interface Firewall (Management Profile Interface)

Selanjutnya kita akan melakukan konfigurasi profile interface management agar interface external yang sudah kita buat tersebut dapat diakses melalui PING, SSH atau HTTPS melalui menu **Network** → **Interface Mgmt** → **Add**, isikan Name profile, Permited Services, Permited IP address untuk interface external, contohnya dapat dilihat pada gambar di bawah

Selanjutnya kita akan melakukan assign profile interface management tersebut kepada interface external melalui menu Network → Interfaces → ethernet1/1< Interface selected> → Advanced → Other Info → Management Profile, contoh seperti gambar di bawah ini

Ethernet	VLAN	Loopback	Tunnel									
<b>L</b>												
Interface		Interfa	асе Туре	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual- Wire	Security Zo	ne	Features Co
•••• ethernel		Layer3	Et	hernet Interface							0	
etherne	t1/2		- F	Interface Name	ethernet1/	1						
ethernel	t1/3		_	Comment							-1	
ethernel	t1/4			Interface Type	Laver3						-	
ethernel	t1/5		_	Netflow Profile	None						~	
ethernel	t1/6			Config IDv4	IDue	Advanced					-	
ethernel	t1//		- 11	COILING IF V4	IFVU	Ruvanceu						
ethernel	E1/8			Link Settings							11	
aaa ethernei	c1/9			Link Speed au	to	Link D	ouplex auto	Link S	tate auto	•		
					0.5.1.1		1100				11	
				Other Into AF	(P Entries	ND Entries NDF	Proxy LLDP				- 11	
				Management	Profile Ex	ternal-Permited				~		
					MTU [5	76 - 1500]						
				🗌 🗌 Adjust TCI	P MSS							
				IPv4 MSS A	djustment	40						
			_	IPv6 MSS A	djustment	60						
						Untagged Subinterfac	e					
									ОК	Cancel		
												1

Bagitu juga konfigurasi dengan interface Internal, silahkan dikonfigurasi sesuai dengan standard sekurity yang diinginkan

# **10.Basic Configuration Policy**

Seperti Biasa, di dalam firewall terdapat policy untuk mengatur secure communication antara interzone maupun intrazone, untuk melakukan konfigurasi Policy dapat dilakukan melalui menu **Policies**  $\rightarrow$  Security  $\rightarrow$  Add, pada contoh kali ini kita akan mencoba melakukan kontrol komunikasi interzone menggunakan policy antara **Zone DMZ menuju Zone Internal**, komunikasi yang diperbolehkan antara DMZ dan Internal Zone adalah Ping dan HTTP, selebihnya akan di Drop, sdangkan dari internal tidak akan dapat melakukan komunikasi kepada DMZ karena kita tidak membuat policy untuk melakukan komunikasi tersebut, contoh sepertibgambar di bawah ini

	Name	Tags	Туре	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Option
1	External-Internal	none	universal	🕅 External	See External-Network	any	any	🕅 Internal	🔙 Internal-Network	🔝 icmp	any	S Allow	none	
										📰 ping				
										web-browsing				
2	DMZ-Internal	none	interzone	pag DMZ	Se DMZ-Network	any	any	🕅 Internal	Seg Internal-Network	📰 ping	any	Allow	none	
										🔛 web-browsing				
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
4	interzone-default	none	interzone	any	any	any	any	any	any	any	any	O Deny	none	none

Testing akan dilakukan melalui host yang berada pada zone DMZ untuk mengakses Host Internal sebagai contohnya di sini host ubuntu DMZ akan mengakses host windows IIS Internal, hasil seperti gambar di bawah ini

#### Test Komunikasi dari DMZ menuju Internal (Allowed PING, WEB)

	lhutapea@SRV-BDG: ~
192 6 packet rtt min, lhutapea eth0	.168.20.100 ping statistics ts transmitted, 6 received, 0% packet loss, time 5006ms /avg/max/mdev = 0.596/1.846/4.149/1.092 ms a@SRV-BDG:~\$ ifconfig Link encap:Ethernet HWaddr 00:0c:29:79:df:9a
	<pre>inet addr:192.168.30.102 Bcast:192.168.30.255 Mask:255.255.255.0 inet6 addr: fe80::20c:29ff:fe79:df9a/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:138 errors:0 dropped:0 overruns:0 frame:0 TX packets:321 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:113825 (113.8 KB) TX bytes:45024 (45.0 KB) Interrupt:19 Base address:0x2000</pre>

lhutapea@SRV-BDG:~\$ route -n Kernel IP routing table													
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface						
0.0.0.0	192.168.30.1	0.0.0.0	UG	0	0	Θ	eth0						
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	eth0						
192.168.30.0	0.0.0	255.255.255.0	U	1	0	0	eth0						

### **Testing: (Allowed)**

PING

_							
ιhι	utapea(	ĝSRV-E	3DG:~\$ ping 192.	168.20.100			
PII	NG 192.	168.2	20.100 (192.168.2	20.100) 56(8	34) bytes	s of data.	
64	bytes	from	192.168.20.100:	icmp_req=1	ttl=127	time=0.576	MS
64	bytes	from	192.168.20.100:	icmp_req=2	ttl=127	time=1.32	ทร
64	bytes	from	192.168.20.100:	icmp_req=3	ttl=127	time=135 m	S
64	bytes	from	192.168.20.100:	icmp_req=4	ttl=127	time=1.47	ทร
64	bytes	from	192.168.20.100:	icmp_req=5	ttl=127	time=1.67	าร
64	bytes	from	192.168.20.100:	icmp_req=6	ttl=127	time=1.77	าร
64	bytes	from	192.168.20.100:	icmp_req=7	ttl=127	time=1.56	ทร

HTTP



Test Komunikasi Dari Internal Menuju DMZ (Not Allowed)

PING

```
Ethernet adapter VMware Network Adapter VMnet2:
Connection-specific DNS Suffix .:
Link-local IPv6 Address . . . . : fe80::199a:cf7e:e3b7:75fe%25
IPv4 Address. . . . . . . . : 192.168.20.100
Subnet Mask . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . : 192.168.20.1
```

Pinging 192.168.30.102 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.30.102: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\Users\LAB-GDI-NE>ping 192.168.30.102

#### HTTP

← → × ① 192.168.30.102		
	Situs ini tidak dapat dijangkau	
	192.168.30.102 membutuhkan terlalu banyak waktu untuk merespons.	
	Coba: Periksa sambungan Memeriksa proxy dan firewall Jalankan Diagnostik Jaringan Windows ERR_CONNECTION_TIMED_OUT	
	Muat ulang	DETAIL

Selanjutnya kita akan mencoba menghapus komunikasi PING dari Zone DMZ menuju Zone Internal kemudian akan melakukan test, hasilnya akan dilampirkan pada contoh gambar di bawah

					Sou	ce		Destination						
	Name	Tags	Туре	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Option
1	External-Internal	none	universal	🕅 External	🔙 External-Network	any	any	🕅 Internal	🔙 Internal-Network	🔢 icmp	any	S Allow	none	
										🏥 ping				
										🔢 web-browsing				
2	DMZ-Internal	none	interzone	(22) DMZ	S DMZ-Network	any	any	🕅 Internal	Si Internal-Network	📰 web-browsing	any	S Allow	none	
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
4	interzone-default	none	interzone	any	any	any	any	any	any	any	any	🛇 Deny	none	none

#### **Policy Remove Communication PING**

Testing :

PING (Not Allowed)



#### HTTP (Allowed)



### **11.Basic Configure NAT**

### a. DNAT

Konfigurasi NAT pertama yang akan kita lakukan adalah DNAT IP Public To Private, dengan tujuan agar web server/aplikasi yang kita miliki pada segment Private address dapat diakses melalui public IP, pada kasus ini kita akan mentranslasikan Ip public 192.168.99.40 agar di translasikan private IIS 192.168.20.100 pada zona Internal, untuk melakukan konfigurasi

NAT pertama kita akan menambahkan address profile untuk IP Public dan IP private IIS melalui menu **Objects**  $\rightarrow$  **Address**  $\rightarrow$  **Add** 

IIS-Private	IP Netmask	192.168.20.100
IIS-Public	IP Netmask	192.168.99.40

Selanjutnya kita akan melakukan konfigurasi Policy NAT UNTUK MENTRANSLASIKAN ip Public ke dalam IP Private melalui menu **Policies**  $\rightarrow$  **NAT**  $\rightarrow$  **Add**, kemudian lakukan konfigurasi seperti contoh gambar di bawah

	Name	🗢 Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	IIS-Access	none	🕅 External	🕅 External	any	any	🔙 IIS-Public	any	none	address: IIS-Private

Source Zone : External Destination Zone : External Destination Interface : Any Destination Address : IIS Public (192.168.99.40) Service : Any Source Translation : None Destination Translation : IIS-Private (192.168.20.40)

Setelah melakukan konfigurasi Policy NAT selanjutnya kita akan melakukan konfigurasi Policy Security untuk mengizinkan komunikasi dari external ke dalam IP Publik Web server IIS melalui menu **Policies** → **Security** Contohnya seperti gambar di bawah ini

	Name	Tags	Туре	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Optio
1	External-Internal	none	universal	(20) External	any	any	any	(22) Internal	😼 IIS-Public	🖽 icmp	any	Allow	none	
										🖽 ping				
										E web-browsing				

Source Zone : External Address : Any User : Any Destination Zone : Internal Destination Address : IIS-Public (192.168.99.40) Application : icmp, PING, Web-browsing Service : Any Action : Allow

Selanjutnya kita akan melakukan koneksi testing pada Konfigurasi NAT yang baru saja kita lakukan melalui IP Public contohnya di sini adalah 192.168.99.0/24

#### PING

```
C:\Users\LAB-GDI-NE>ping 192.168.99.40
Pinging 192.168.99.40 with 32 bytes of data:
Reply from 192.168.99.1: Destination port unreachable.
Reply from 192.168.99.40: bytes=32 time=2ms TTL=127
Reply from 192.168.99.40: bytes=32 time=1ms TTL=127
Ping statistics for 192.168.99.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```



#### Access Web



#### b. SNAT

Konfigurasi SNAT biasa kita gunakan untuk koneksi internal network menuju public IP address (Internet), atau biasa dikenal dengan NAT Overload, berikut adalah contoh konfigurasi NAT overload di palo alto

Pertama create policy security Internal network menuju internet melalui menu Policies  $\rightarrow$  Security, buatlah policy seperti yang dapat dilihat pada contoh gambar di bawah ini

2 Security Inet 🔹 none universal 🎮 Internal 😽 Internal-Netw... any any 🎮 External any any any even any even

Source Zone : Internal Source Address : Internal Network (192.168.20.0/24) Source User : Any Destination Zone : External Destinatopn Address : Any Action : Allow

Selanjutnya kita akan melakukan konfigurasi security NAT melalui menu **Policies**  $\rightarrow$  **NAT** Untuk konfigurasi NAT Overload / Source NAT, lakukan konfigurasi security NAT seperti contoh gambar di bawah ini



Name : SNAT-INET Source Zone : Internal Destination Zone : External Destination Interface : ethernet1/1 Source Address : Internal-Network (192.168.20.0/24) Destination Address : Any Service : Any Translation type : dynamic IP and Port Address Type : Interface Address Interface : ethernet1/1 IP address : External (192.168.99.80)

Dan yang terakhir adalah pastikan kita sudah memiliki default route kepada gateway yang benar, untuk melakukan konfigurasi default route kita dapat melalui menu Network  $\rightarrow$  Virtual Router  $\rightarrow$  Default  $\rightarrow$  Static Route  $\rightarrow$  Add, contoh dapat dilihat pada gambar berikut ini

	Virtual Router - default	•	
Name	Router Settings Static Routes	IPv4 IPv6	Multicast
	Redistribution Profile RIP OSPF	Virtual Route - IPv4	
	OSPFv3 BGP Multicast	Next Hop  IP Address Next VR Discard None  I92.168.98.1  Admin Distance 10 - 240  Metric 10  No Install	
		BFD Profile None	

# **12.Basic Konfigurasi Global Protect**

Global protect adalah remote access VPN yang dimiliki oleh Palo Alto Firewall, Pada sesi ini kita akan melakukan konfigurasi Global Protect pada palo alto virtual agar remote host bisa melakukan access kepada internal network melalui VPN,

1. Tahap pertama lakukan konfigurasi **User local database** melalui menu **Device** → **local user database** → **Users,** kemudian lakukan pengisian nama user beserta password Untuk user yang dapat menggunakan VPN

Name	Ihutapea
Mode	Password O Password Hash
Password	•••••
Confirm Password	•••••
	✓ Enable
	OK Cancel

 Pada interface External (Public) yang akan dijadikan remote gateway VPN lakukan konfigurasi VPN Tunnel interface melalui menu Network → Interface → Tunnel seperti gambar di bawah ini,

Ma	Tunnel Inte	erface				0	ment
PT	In	terface Name			. 2		
		Comment					
	N	etflow Profile	None				_
	Config	IPv4 IPv	v6 Advanced				
	Assig	n Interface T	D				
		Virtual Rout	er default				
		Security Zor	ne Corp-VPN			~	
					ОК	Cancel	

Isi interface number tunnel pada gambar contoh **tunnel 2** pada virtual router pilih **default** pada security zone buatlah security zone khusus Remote VPN, pada contoh gambar saya berikan nama **Corp-VPN** contoh konfigurasi **zone security VPN** dapat dilihat pada gambar berikut

Zone		ତ
Name	¢orp-VPN	User Identification ACL
	Service Profile Zone for NSX	Indude List 🔺
Туре	Layer3	Select an address or address group or type in your own
🔲 Interfaces 🔺		address, EX: 192.108.1.20 or 192.108.1.0/24
tunnel.2		
		🛨 Add 🗖 Delete
		Users from these addresses/subnets will be identified.
		Exclude List 🔺
🕂 Add 🗖 Delete		Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Zone Protection Profile	None	
Log Setting	None	🕂 Add 💭 Delete
	Senable User Identification	Users from these addresses/subnets will not be identified.
		OK Cancel

 Create authentication profile Remote VPN melalui menu Device → Authentication Profile, di sini saya menggunakan authentikasi dengan user database local, dengan contoh konfigurasi seperti gambar di bawah

Lockout	
Loca Authentication Profile	💿 i <mark>erver Profile</mark>
Name LOCAL	
Authentication Advanced	
Type Local Database	<b>v</b>
User Domain	
Username Modifier %USERINPUT%	<b>v</b>
— Single Sign On —	
Kerberos Realm	
Kerberos Keytab Click "Import" to configure this field	X Import
	OK Cancel

Authentication Profile	0
oca Name LOCAL	erver Pro
Authentication Advanced	
Allow List	
Allow List	
afachry	
S Ihutapea	
Account Lockout	
Failed Attempts 0	
Lockout Time (min) 0	
OK	cel

Klik Add untuk menambahkan list user yang dapat melakukan remote access VPN pada contoh saya mendaftarkan nama **lhutapea** dan **afachry** untuk dapat melakukan remote access VPN

 Selanjutnya kita akan melakukan konfigurasi GlobalProtect Gateway profile melalui menu Network → GlobalProtect → Gateways kemudian lakukan konfigurasi seperti gambar di bawah ini

GlobalProtect Gate	way Configuration		0
General	Name G	w-Global-protect	٦
Authentication	Network Settings		
Agent	Interface	ethernet1/1	
Agent	IP Address	External	
Satellite			
		OK	

Isikan nama profile GlobalProtect gateway kemudian Pada network setting pilih interface External yang akan dijadikan remote access gateway VPN, dan pilih IP address yang dimiliki oleh interface external.

GlobalProtect Gate	way Configuration			Ø
General	Server Authentication			
Authentication	SSL/TLS Service Profile Cert	-VPN		<b>V</b>
Agent	Client Authentication			
Satellite	Name	os	Authentication Profile	Authentication Message
	Local	Any	LOCAL	Enter login credentials
	Add      Delete     Olone     Certificate Profile     None	Move Up  Move Down		
				OK Cancel

Pada menu Authentication lakukan konfigurasi seperti berikut ini

Pada server authentication pilih **SSL/TLS service profile** atau jika belum ada silahkan melakukan create dengan melakukan drop down profile dan memilih menu new seperti gambar di bawah ini

21	GlobalProtect Gate	eway Configuration			0	
a	General	Server Authentication				
	Authentication	SSL/TLS Service Profile	Cert-VPN	-		
			Cert-VPN			
Agent	Agent	Client Authentication	New 🚆 SSL/TLS Service Profile			
	C					

GlobalProtect Gate	way Configuration			0
General Authentication	Server Authentication SSL/TLS Service Profile Cer	t-VPN		
Agent	Client Authentication			
Satellite	Name			Authentication Message
	SSL/TLS Service Nam Certificat Protocol Setti Min Ver Max Ver	Profile e Cert-VPN e   GCA-GlobalProtect sio New 🛓 Import 👼 Ger sion Max	erate	
	c	l	OK Cancel	<b>V</b>
				OK Cancel

### Selanjutnya islah profile seperti contoh gambar di bawah ini

Pada pilihan certificate silahkan pilih certificate profile yang sudah kita miliki melalui pilihan drop down menu dengan memilih menu **import** atau jika kita belum memiliki silahkan pilih **generate** untuk melakukan generate certificate kita sendiri, contoh cara melakukan generate certificate dapat dilihat pada gambar di bawah ini

	Generate Certificate		0	
	Certificate Type	Local O SCEP		
	Certificate Name	A-GlobalProtect		
cat	Common Name 1	92.168.98.125		
	IP	or FQDN to appear on the certificate		
-	Signed by	Certificate Authority	· ·	res
2	OCSP Responder		-	3 07:56:21 2018
	Cryptographic Set	tings		
	Algorithm	RSA	-	
	Number of Bits	2048	~	
	Digest	sha256	~	
	Expiration (days)	365		
	Certificate Attributes	;	- 1	
	🗖 Туре	Value		
	🕂 Add 🗖 Delete			
rate		Generate	ncel	

Pada **Common name** isikan IP address interface external atau FQDN address yang dimiliki IP Address external tersebut sebagai remote access gateway globalprotect Lakukan **centang pada Certificate Authority**, certificate profile di atas dan dapat kita generate secara manual melalui menu **Device** → **Crertificate** → **Generate** 

Pada **Client Authentication** lakukan Add profile pada contoh gambar saya membuat profile dengan nama local untuk authentikasi local dan pada colom **Authentication Profile** saya memilih authentikasi **LOCAL Profile** yang sudah saya create sebelumnya



Pada menu agent kita harus melakukan konfigurasi pada menu **Tunnel Setting**, **Client Setting**, **dan network setting**. Pada konfigurasi tunnel setting dapat dilihat pada gambar di bawah ini

ne.		Location Local In	itertace Local	þ	unnel May Liser					
-Gl	GlobalProtect Gate	eway Configuration			Ø					
	General	Tunnel Settings Timeout	Sattings Client Sattings	Natwork Sanicas HIP	Notification					
	Authentication	Tunner Settings	Jetunga Gient Jetunga	THE WORK SET WILES THI	Notification					
	Agent	Tunnel Mode								
	Agent	Tunnel Interface	tunnel.2		<b>v</b>					
	Satellite	Max User	[1 - 25]							
			Inable IPSec							
		GlobalProtect IPSec Crypto	default							
			Enable X-Auth Support							
		Group Name								
		Group Password								
		Confirm Group Password								
			Skip Auth on IKE Rekey							
		1								
					OK Cancel					

Lakukan centang pada **Tunnel Mode** dan tentukan interface tunnel yang akan dijadikan tunnel interface remote access VPN pada contoh kita menggunakan

**tunnel.2** yang telah kita create sebelumnya, lakukan centang pada **Enable IPsec** dan pada GlobalProtectIPsec Crypto pilih **default** saja, pada **Client Setting** kita akan melakukan konfigurasi IP Pool VPN Setting, contoh dapat kita lihat pada gambar di bawah ini

GlobalProtect Gateway Configuration									
	General	Tu	nnel Settings	Timeout Settings	Client Settings	Network Services	HIP Notification		
Authentication								1 item 🔿 🗙	
	Satellite		Configs	User/User Group	os	IP Pool	Authentication Server IP Pool	Access Route	
I			VPN-Global	any	any	192.168.20.50-19			

1	Configs						0	ser
IC	Authentication Overric	le User/User G	iroup	Network Settings				0
G	Name VF	N-Global					1	
A	Authentication Ov	erride						h
A			Gene	erate cookie for auth	entication override			
5		Cookie Lifetime	Hours		24			
l	Certificate to Epor	unt/Decrunt Cookie		pt cookie for authen	tication override	~		
I	Certificate to End	уруреа урт сооме	CA-GIODA	airtotect				
ľ								
						OK Cancel	J	
h								

Pada Certificate to Encryp/Decrypt Cookie silahkan pilih certificate profile CA yang telah kita buat sebelumnya contoh di sini adalah **CA-GlobalProtect** 

	Configs		0 <sub>000</sub>
Glo	Authentication Override User/User Group	Network Settings	
G	any	🜌 Any	
A	Source User 🔺	os 🔺	
A			
S			
	🕈 Add 🗖 Delete	Add. 💭 Delete	- 11
		ок са	ancel

Pada menu User/User group kita biarkan saja default yaitu any user dan any OS, pada network setting lakukan konfigurasi IP Pool Access VPN yang akan didaptkan client ketika melakukan remote access VPN , pada contoh di bawah sya menggunakan segment internal 192.168.20.50-192.168.20.100

	Configs	0
Glo	Authentication Override User/User Group Network Settings	
G	Retrieve Framed-IP-Address attribute from authentication server	No direct access to local network No direct access to local network is applicable to Windows and Mac only
Ĥ	Authentication Server IP Pool	Access Route
S	Enter IP subnets or ranges (e.g. 192.168.74.0/24, 192.168.75.1-192.168.75.100) to match the Framed IP attribute of the authentication server.	Enter subnets need to be accessed by dients (e.g. 172.16.1.0/24)
	Add 🗢 Delete	
	These IPs will be added to the firewall's routing table	
	IP Pool	
l	192. 168. 20. 50-192. 168. 20. 100	
	🕂 Add 🗖 Delete 🔕 Mave Up 🗳 Mave Down	+ Add Delete
	These IPs will be added to the firewall's routing table	These routes will be added to the client's routing table
		OK Cancel

Pada network setting kita akan melakukan configurasi DNS address yang akan di dapatkan remote access vpn client ketika melakukan koneksi VPN ke palo alto, contoh dapat dilihat pada gambar di bawah

GlobalProtect Gate	eway Configuration						(
General							
Authentication	Tunnel Settings	Timeout Settings	Client Settings	Network Services	HIP Notificatio	n	
	Inheritance Source	None				-	
Agent	Agent <ul> <li>Check inheritance source status</li> </ul> <ul> <li>Satellite</li> <li>Primary DNS</li> <li>8.8.8</li> </ul> <ul> <li>Satellite</li> <li>Primary DNS</li> <li>8.8.8</li> </ul> <ul> <li>Satellite</li> <li>Satellite</li> <li>Satellite</li> <li>Satellite</li> </ul> <ul> <li>Satellite</li> <li>Satellite</li> <li>Satellite</li> </ul> <ul> <li>Satellite</li> <li>Satellite</li> <li>Satellite</li> <li>Satellite</li> <li>Satellite</li> <li>Satellite</li> <li>Satellite</li> </ul>						
Satellite							
	Secondary DNS	8.8.4.4					~
	Primary WINS	None				-	~
	Secondary WINS	None				-	~
	DNS Suffix	Enter comma-separat	ted DNS suffix for die	nt (e.g. hr.mycompany	com, mycompany.	com)	
		Inherit DNS Suffix	es				
					ſ	OK Cancel	
					U U		

 Selanjutnya kita akan melakukan konfigurasi GlobalProtect Portal melalui menu Network → GlobalProtect → Portals, contoh profile dapat dilihat seperti gambar di bawah

Name		Location Inter	ace	IP	SSL/TLS Service Profi	le Authentication Pr	ofile Certificate Profi
] Portal	GlobalProtect Por	tal Configuration					0
	General	Nar	Portal-Global				
	Authentication	Network Settings					
	Agent	Interfa	ce ethernet1/1				<b>v</b>
	rigone	IP Addre	ss External				<b>v</b>
	Satellite	Appo2#2000					
		Appearance	🗌 Disable login p	bage			
		Custom Login Pa	ge factory-default				V
		Custom Help Pa	ge factory-default				V
						ок	Cancel

Pada General config silahkan isi **nama profile** GlobalProtect Portal, **interface** yang akan digunakan sebagai gateway portal, pada contoh saya memilih **external interface public**, pada **Custom Login Page** dan **Help Page** pilih **Factory default saja** Pada menu authentikasi contoh konfigurasi terlihat pada gambar di bawah ini

rtal	GlobalProtect Port	tal Configuration				0			
	General Authentication	SSL/TLS Service Prof	Server Authentication SSL/TLS Service Profile Cert-VPN						
	Agent	Client Authentication							
	Satellite	Name	os	Authentication Profile	Authentication Message				
		Add Certificate Prof	Any Clone O Move Up O M	love Down	Enter login credentiais	<b>•</b>			
0					OK Cano	:el			

Hamper sama dengan GlobalProtect Gateway pada **Server Authentication** pilih SSL/TLS service profile, pada contoh saya menggunakan certificate yang sudah kita create sebelumnya yaitu **Cert-VPN** kemudian pada **Client Authentication** silahkan create profile client authentication, pada contoh gambar saya membuat profile

dengan nama **LOCAL** dengan authentication method profile yaitu **LOCAL**. Pada menu **Agent** silah kan lakukan konfigurasi **Agent Profile** seperti contoh gambar di bawah ini

Name Portal	GlobalProtect Porte	al Configuration					0
	General	Agent					
	Authentication	Configs	User/User Group	OS	External Gateways	Client Certificate	
	Agent	Portal	any	any	Portal-VPN (Highest)	local	
	Satellite						
		🕂 Add 🗖 Delete 📀 (	Clone 🖸 Move Up 🖸 Move Dow	n			
		Trusted Root CA	Install in Local Root		Agent User Override Key	••••	1
			Certificate Store	Con	firm Agent User Override Key	••••	
		<b>0</b>		- 11			
		🛨 Add 🕒 Delete					
<b>D</b>							
9.30						OK Cancel	

Pada gambar di bawah ini adalah contoh configurasi profile menu **agent** pada GlobalProtect Portal.

	Configs							0
-	Authentication	User/User Group	Gateways	Арр	Data	a Col	ection	
me		Name	Portal					
		Client Certificate	Local			▼	CA-GlobalProtect	-
			The selected client	t certificate	including	j its p	ivate key will be installed on client machines.	
	Save User Credentials Yes							•
	Authentication Override							
	Generate cookie for authentication override							
		Cookie Lifetime	Hours 24					
			Accept coo	kie for au	thentic	ation	override	
	Certificate to E	ncrypt/Decrypt Cookie	None					~
	Turn Frankru A							_
	- Two-Factor A							
		Portal authent	ication				Manual only external gateway authentication	
		Internal gatew	ay authenticati	on			Auto discovery external gateway authentication	
	Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.							
							ОК Сапсе	4

Silahkan isi name profile Agent authentication, dan **Client Certificate** yang akan digunakan client ketika melakukan access remote VPN pada contoh saya

menggunakan profile certificate yang sudah kita generate sebelumnya yaitu **CA-GlobalProtect,** pada user group menu saya biarkan saja default untuk any user dan any OS seperti gambar di bawah

I	Configs							0	
1	Authentication	User/User Group	Gateways	Арр	Data Collection				
ne tal	🗹 Any				any	~			lerun
	OS 🔺				User	/User Group 🔺			
								_	
	🛨 Add 🖃 Dele	te			Add 🕈	Uelete			
							ОК	Cancel	

Pada konfigurasi menu gateways dapat dilihat pada gambar di bawah ini

	Configs										0	l
-	Authentication	User/User Group	Gateways	Арр	Da	ata Collection						
me rtal	Internal Gate	eways				– External Gat	teways					
Т						Cutoff Tin	ne (sec)	5				
	Name	Addre				Name		Address 🔺	Priority	Manual		
						Portal-VPN		192.168.98.152	Highest			
	Add O	lelete 🖸 Move Up 🖸	Move Down			🕈 Add 🗖	Delete					
	TD Add	troop			, I	Third Party VPN						
	Hostn	name			1							
					1							
						🛨 Add 🔳 De	lete					
										OK Cance	2	

Yang perlu kita isi adalah **External Gateway**, saya telah membuat external gateway profile dengan nama **Portal-VPN** dengan menggunaka IP address External Public yaitu IP yang akan diakses agent ketika melakukan VPN remote access, pada menu **App** saya melakukan konfigurasi seperti pada contoh gambar di bawah ini

Configs									0
Authentication	User/User Gro	oup Gateways	Арр	Data Co	ollection				
App Configu	rations				Dicab	Welcome Page	None		~
Connect Met	hod	On-demand (Manu initiated connectio	ial user n)	Â	Disabi	le GiobalProtect App			
GlobalProtect Refresh Inter	App Config val (hours)	24 [1 - 168]		=		Passcode			
Allow User to GlobalProtect	Disable	allowed		_		Confirm Passcode	•		
Allow User to GlobalProtect	Upgrade App	prompt			Max	Disable Timeout (min)	0		
Use Single Sig Only)	n-on (Windows	Yes			- Mobile	e Security Manager 9	Settinas —		
Clear Single S on Logout (W	ign-On Credentials indows Only)	Yes				Mobile Security Manage	er		
Use Default A Kerberos Aut (Windows On	uthentication on hentication Failure ly)	Yes				Enrollment Po	rt 443		V
Client Certific	ate Store Lookup	user-and-machine							
SCEP Certific (days)	ate Renewal Period	7 [0 - 30]							
Extended Ker	Instant       Out, Out, out, out, out, out, out, out, out, o								
					_]				
								ок	Cancel
		Delote							

Pada gambar di atas saya hanya melakukan perubahan pada Connected Method menjadi On-Demmand

ame ortal-	GlobalProtect Port	tal Configuration						0
	General	Satellite						
	Authentication	Name	Configuration Refresh Interval	Satellite Hostname	Serial Number	External Gateways	Routing Priority	
	Agent		(hours)					
	Satellite							
		+ Add - Delete Avve Up S Move Dawn						
		Client Certificate  CLocal  SCEP						
					Issuing Certificate	None		-
					OCSP Responder	None		~
				V	/alidity Period (days)	7		_
		🛨 Add 🗖 Delete		Certificate Re	newal Period (days)	3		_
ÐD								
30							OK Can	cel

Pada Menu Satelite kita akan membiarkanya sebagai default konfigurasi

Sampai disini kita telah melakukan semua tahap yang dibutuhkan untuk melakukan konfigurasi remote access VPN Pada Palo Alto, selanjutnya kita akan melakukan testing pada client.

### 6. Testing

Pada tahap ini kita akan mencoba melakukan akses remote VPN melalui GlobalProtect yang dimiliki oleh palo alto, pertama-tama kita akan melakukan akses kepada globalProtect portal yaitu IP address external palo alto yang sudah kita tentukan sebagai Gateway GlobalProtect dan access portal, akses globalprotect portal melalui browser dengan mengetikkan IP address atau FQDN addres tersebut

o 📙 Fortinet 🔒 PMP ы FP	
t Portal	
-	t Portal

Selanjutnya lakukan login menggunakan user yang sudah kita daftarkan sebelumnya ke dalam local user database, setelah login maka selanjutnya kita akan diperintahkan untuk melakukan download aplikasi GlobalProtect Agent agar dilakukan install kepada laptop atau local PC kita, contoh seperti gambar di bawah ini



Setelah melakukan download, lakukan instalasi agent aplikasi ke dalam local host kita, setelah terinstall maka aplikasi agent dapat kita lihat sepeti contoh gambar di bawah ini

GlobalProtect	et calcolto	
Home Details Ho	it State Troubleshooting	
Portal:	192.168.98.152	
Username:	hutapea	
Password:	******	
	Connect Clear	
Status: Not Cor	inected	
-Warnings/Errors -		
	Mac OS needs to download a	and
	install Mac 32/64 bit GlobalP	rotect
Selanjutnya lakukan koneksi VPN melalui aplikasi GlobalProtect Agent hingga berhasil menginstal certificate SSL dan mendapatkan retriving informasi serta **connected status** seperti contoh gambar dibawah

Ser	ver Certificate Error	General Details Certification Path
l Usei Pas Status:	There is a problem with the s 192. 168.98.152 cannot be v organization to have the issu Warning: The communication compromised. We recommen- connection. Error details: The 192.168.98.152 certifica authority	Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Warnings Resend c	distant,	Issued to: 192.168.98.152
	Show Certificate	Issued by: 192.168.98.152
	N 00	Valid from 7/ 13/ 2017 to 7/ 13/ 2018
	Mac US needs install Mac 32/0 agent.	Install Certificate Issuer Statement

C GlobalProtect	
Home Details Host State Troubleshooting	
Portal: 192.168.98.152	
Username: Ihutapea	
Password: ********	
Clear	
Status: Connected	
Warnings/Errors	
Mac OS poods to download and	

Jika kita sudah terkoneksi kita akan mendapatkan IP address Pool VPN yang dapat kita lihat melalui menu detail

ome Details Host	State   Trout	oleshooting				
Connection						
Portal:	19	92.168.98.152				
Assigned Local IP	: 19	92.168.20.50				
GlobalProtect Ga	teway IP: 19	92.168.98.152				
Protocol:	IP	Sec				
Statistics						
Bytes In:	3,480	Bytes Out:	54,915			
Packet In:	58	Packet Out:	353			
Packet I/Error:	0	Packet O/Erro	or: 3			
Cataway	Tree	Turnel	Authoritizated	Linking	Deserved Sur	Magual
Gateway	External	iunnei		Uptime	Password Exp	Manual
192,100,90,132	External	165	105	00.00.30	19/A	10
4						

Katika sudah terkoneksi ke dalam IP local VPN selanjutnya kita dapat mengakses local IP server seperti Apche server berikut yang berada pada IP 192.168.20.102



This is the default web page for Server BANDUNG.

The web server software is running but no content has been added, yet.

Tracing	route to	192.168.2	20.102	over a maximum of 30 hops
1 2	* 6 ms	* 7 ms	* 5 ms	Request timed out. 192.168.20.102
Trace co	omplete.			
C:\Users	s∖admin>			

# **13.Basic Konfigurasi Split Tunneling**

Untuk melakukan konfigurasi split tunneling kita dapat menambahkan specific segment Access Route ke dalam client setting profile agar ketika client melakukan akses remote VPN melalui palo alto segment tersebut saja yang akan di tambahkan ke dalam routing table client agar dilewatkan melalui tunnel, sedangkan segment yang lain seperti internet dapat melalui gateway host itu sendiri, contoh konfigurasi plit tunneling dapat dilakukan melalui menu Network  $\rightarrow$  GlobalProtect Gateway  $\rightarrow$  < Global Protect profile>  $\rightarrow$  Client Setting  $\rightarrow$ <Profile>  $\rightarrow$  Network Setting  $\rightarrow$  Access Route. Contoh dapat dilihat sepeti gambar di bawah ini

Name	Configs			0	lser
Gw-Gl Glc	Authentication Override	User/User Group	Network Settings		0
G	Retrieve Framed-IP-Addr	ress attribute from autho	entication server	No direct access to local network No direct access to local network is applicable to Windows and Mac only	Π
A	Authentication Server I	P Pool 🔺		Access Route	
A	Enter IP subnets or ranges	(e.g. 192.168.74.0/24,		192.168.20.0/24	
s	192.168.75.1-192.168.75.	100) to match the Fram	ed IP attribute of	192.168.30.0/24	
	ale dualentied on server.				
	🛨 Add 🗖 Delete				
	These IPs will be added to the fire	ewall's routing table			
	IP Pool				
	192.168.50.50-192.168	8.50.100			
		ove up 💟 Move Down			
	These IPs will be added to the fire	ewall's routing table		These routes will be added to the client's routing table	
				OK Caprel	
26:25				Cancer	

Pada contoh di atas saya menambahkan segment 192.168.20.0/24 dan 192.168.30.0/24 agar dapat dilewatkan melalui tunnel global protect, sedangkan segment yang lain dapat dilewatkan melalui local gateway host, IP pool yang saya gunakan yaitu 192.168.50.50-192.168.50.100, dengan split tunneling kita dapat mengakses remote segment melalui split tunneling dan dapat melakukan akses internet melalui local gateway kita sendiri.

======================================				=====
Active Routes:				
Network Destination	n Netmask	Gateway	Interface	Metric
0.0.0	0.0.0.0	192.168.98.1	192.168.98.140	25
8.8.4.4	255.255.255.255	On-link	192.168.50.50	1
8.8.8.8	255.255.255.255	On-link	192.168.50.50	1
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
169.254.0.0	255.255.0.0	On-link	169.254.187.236	286
169.254.0.0	255.255.0.0	On-link	169.254.191.208	276
169.254.187.236	255.255.255.255	On-link	169.254.187.236	286
169.254.191.208	255.255.255.255	On-link	169.254.191.208	276
169.254.255.255	255.255.255.255	On-link	169.254.187.236	286
169.254.255.255	255.255.255.255	On-link	169.254.191.208	276
192.168.20.0	255.255.255.0	On-link	192.168.50.50	1
192.168.20.255	255.255.255.255	On-link	192.168.50.50	256
192.168.23.0	255.255.255.0	On-link	192.168.23.1	276
192.168.23.1	255.255.255.255	On-link	192.168.23.1	276
192.168.23.255	255.255.255.255	On-link	192.168.23.1	276
192.168.30.0	255.255.255.0	On-link	192.168.50.50	1
192.168.30.255	255.255.255.255	On-link	192.168.50.50	256
192.168.50.50	255.255.255.255	On-link	192.168.50.50	256
192.168.98.0	255.255.255.0	On-link	192.168.98.140	281
192.168.98.140	255.255.255.255	On-link	192.168.98.140	281
192.168.98.152	255.255.255.255	On-link	192.168.98.140	281
192.168.98.255	255.255.255.255	On-link	192.168.98.140	281
224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	192.168.98.140	281
224.0.0.0	240.0.0.0	On-link	169.254.191.208	276
224.0.0.0	240.0.0.0	On-link	192.168.23.1	276
224.0.0.0	240.0.0.0	On-link	169.254.187.236	286
224.0.0.0	240.0.0.0	On-link	192.168.50.50	256
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	192.168.98.140	281
255.255.255.255	255.255.255.255	On-link	169.254.191.208	276
255.255.255.255	255.255.255.255	On-link	192.168.23.1	276
255.255.255.255	255.255.255.255	On-link	169.254.187.236	286
255.255.255.255	255.255.255.255	On-link	192.168.50.50	256
=======================================	=========================		====================	======
Persistent Routes:				
None				

# 14.Konfigurasi Palo Alto Join AD (Agentless)

Dalam melakukan integrasi Palo Alto Firewall ke Active Directory terdapat beberapa langkah yang harus diperhatikan untuk dapat melakukan integrasi ke dalam active directory

 Create User AD untuk digunakan palo alto dalam melakukan join active directory Pada contoh ini saya menggunakan active directory pada win server 2012 R2 Buatlah user AD dengan spesifikasi sebagai berikut melalui menu Server Manager → Tools → Active Directory Users and Computers kemudian buatlah account seperti pada contoh gambar di bawah

	paload	Properties	?	x
Remote control	Remote D	esktop Services Pro	ofile COI	M+
Member Of	Dial-in	Environment	Session	ns
General Address	s Account	Profile Teleph	ones Organiz	ation
	,			
User logon name:				_
paload		@galaxidata.loca	al	<b>~</b>
User logon name (p	re-Windows 2000	D):		
GALAXIDATA\		paload		
	1			
Logon Hours	Log On To	D		
r				
Unlock account				
Account options:				_
User must cha	ange password at	t next logon		^
User cannot o	hange password			
Password nev	ver expires			
Store passwo	rd using reversibl	e encryption		~
- Account expires -				_
Never				
	00 Contomber (	2017		
	us september /	2017	<u></u>	
			- LL	l.
	UK C	ancel Ap	DIY He	яр
RVER1 4013 Wa	rning Microso	ft-Windows-DNS-	Server-Service	•

Selanjutnya berikan access member permission seperti contoh gambar di bawah ini

	paload	Propert	ties	? X	
Remote control	Remote D	esktop Se	rvices Profile	COM+	
General Address	Account	Profile	Telephones	Organization	
Member Of	Dial-in	Envi	ronment	Sessions	
Member of:					
Name	Active Directo	ory Domain	Services Folde	r	
Distributed COM	galaxidata.loc	al/Builtin			
Domain Users	galaxidata.loo	al/Users			
Event Log Readers	galaxidata.loo	al/Builtin			
Server Operators	galaxidata.loo	al/Builtin			
Add Remove					
Primary group: D	omain Users				
Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.					
0	КС	ancel	Apply	Help	

- Distributed COM
- Event Log Readers
- Server Opertor

Member group ini diperlukan karena jika tidak maka akan muncul status **Access Denied** pada **Server Monitoring** pada saat melakukan konfigurasi WMI Authentication

Langkah selanjutnya kita akan memberikan WMI permission pada user tersebut melalui menu WMI Controll melalui perintah pada RUN "wmimgmt.msc" kemudian pada profile WMI control klik kanan Properties → Security explore folder Root dan pilih folder CIMV2 → Security seperti pada gambar di bawah ini



Selanjutnya tambahkan username yang akan digunakan palo alto untuk integrasi kedalam AD dengan mengklik tombol **Add** pada contoh saya menggunakan <u>paload@galaxidata.local</u> kemudian berikan permission sesuai dengan pada gambar di bawah ini

Console Root	Windows Management Instrumentation (WMI)
	Configur WMI Control (Local) Properties ? ×
	General Backup/Restore Security Advanced
	N Security for ROOT\CIMV2
	Security
	A amar fachry (afachry@galaxidata.local)
	Administrators (GALAXIDATA\Administrators)
	Add
	Permissions for paload Allow Deny
	Provider Write
	Read Security     ✓     □       Edit Security     ✓     □
	For special permissions or advanced settings, Advanced
	OK Cancel Apply

- Enable account
- Remote Enable
- Read Security

Jika kita ingin mengetahui administrative domain name pada active directory gunakan perintah pada run "adsiedit.msc" maka akan muncul jendela **ADSI Edit**, klik kanan pada profile **ADSI Edit** kemudian connect to maka akan muncul jendela seperti di bawah

2			ADSI Edit
File Action View Help			
🗢 🔿 🙍 📰 🗙 🗟 🖻	?		
📝 ADSI Edit	Name	Class	Distinguished Name
a 📋 Default naming context [Sen	CN=Administrator	user	CN=Administrator, CN=Users, DC=galaxidata, DC=local
🛛 🧮 DC=galaxidata,DC=local	CN=Allowed RODC Passwo	group	CN=Allowed RODC Password Replication Group, CN=Users, DC=gal
CN=Builtin	CN=Cert Publishers	group	CN=Cert Publishers, CN=Users, DC=galaxidata, DC=local
CN=Computers	📔 CN=Cloneable Domain Co	group	CN=Cloneable Domain Controllers, CN=Users, DC=galaxidata, DC=Ic
OU=Domain Control	CN=Denied RODC Passwor	group	CN=Denied RODC Password Replication Group, CN=Users, DC=gala:
OU=Engineer OU	CN=DnsAdmins	group	CN=DnsAdmins,CN=Users,DC=galaxidata,DC=local
OU=Finance	CN=DnsUpdateProxy	group	CN=DnsUpdateProxy, CN=Users, DC=galaxidata, DC=local
CN=ForeignSecurityF	📔 CN=Domain Admins	group	CN=Domain Admins,CN=Users,DC=galaxidata,DC=local
CN=LostAndFound	CN=Domain Computers	group	CN=Domain Computers,CN=Users,DC=galaxidata,DC=local
CN=NTDS Ouotas	CN=Domain Controllers	group	CN=Domain Controllers,CN=Users,DC=galaxidata,DC=local
CN=Program Data	🚞 CN=Domain Guests	group	CN=Domain Guests, CN=Users, DC=galaxidata, DC=local
CN=System	📔 CN=Domain Users	group	CN=Domain Users, CN=Users, DC=galaxidata, DC=local
CN=TPM Devices	CN=Enterprise Admins	group	CN=Enterprise Admins,CN=Users,DC=galaxidata,DC=local
CN=Users	CN=Enterprise Read-only D	group	CN=Enterprise Read-only Domain Controllers, CN=Users, DC=galaxi
	CN=Group Policy Creator O	group	CN=Group Policy Creator Owners, CN=Users, DC=galaxidata, DC=loc
	CN=Guest	user	CN=Guest, CN=Users, DC=galaxidata, DC=local
	📫 CN=krbtgt	user	CN=krbtgt,CN=Users,DC=galaxidata,DC=local
	🚞 CN=paload	user	CN=paload, CN=Users, DC=galaxidata, DC=local
	CN=Protected Users	group	CN=Protected Users, CN=Users, DC=galaxidata, DC=local
	CN=RAS and IAS Servers	group	CN=RAS and IAS Servers, CN=Users, DC=galaxidata, DC=local
	📔 CN=Read-only Domain Co	group	CN=Read-only Domain Controllers, CN=Users, DC=galaxidata, DC=k
	🚞 CN=Schema Admins	group	CN=Schema Admins,CN=Users,DC=galaxidata,DC=local
	CN=WinRMRemoteWMIUs	group	CN=WinRMRemoteWMIUsers_,CN=Users,DC=galaxidata,DC=loca
			Activate

Info ini akan berguna saat kita membutuhkan canonical domain name pada user profile pada saat melakukan join AD melalui configurasi profile authentikasi server pada appliance palo alto

Sampai di sini konfigurasi user profile AD yang akan digunakan palo alto untuk integrasi kedalam active directory sudah selesai, selanjutnya kita akan melakukan konfigurasi profile Authentikasi server pada appliance Palo Alto Firewall

Beberapa point penting sebelum melakukan join AD pada perangkat palo alto hal yang perlu diperhatikan adalah

- 1. Komunikasi yang dilakukan appliance palo alto kepada AD local adalah melalui IP Management, pastikan IP management palo alto dapat berkomunikasi kepada active directory
- 2. Pastikan Domain Name, IP DNS server, dan NTP server menggunakan IP Address Active Directory Local
  - a. Untuk domain name melalui menu **Device**  $\rightarrow$  **Management**  $\rightarrow$

General Settings		0
Hostname	PA-VM-Galaxi	
Domain	galaxidata.local	
Logia Ranner	Accept DHCP server provided Hostname     Accept DHCP server provided Domain     This is Drivets Emvironment, even thing you will do use	
Login Banner	alaways monitor	
SSI /TLS Sancisa Brafila		
Time 7and		
Time Zone	Asia/Jakarta	-
Locale	en	-
Date	2017/08/10	-
Time	16:11:18	
Latitude		
Longitude		
	Automatically Acquire Commit Lock	
	Certificate Expiration Check	
	Use Hypervisor Assigned MAC Addresses	
	OK Cance	

b. Untuk IP DNS server dan NTP dapat melalui menu Devices → Services → I Kemudian setting seperti gambar di bawah ini, pada contoh di sini IP AD server adalah 192.168.1.44

Services		0
Services NTP		
DNS (	Servers ODNS Proxy Object	
Primary DNS Server	192.168.1.44	
Secondary DNS Server	8.8.8	
Update Server	updates.paloaltonetworks.com	
(	Verify Update Server Identity	
Proxy Server		
Serv	/er	
P	ort [1 - 65535]	
U	ser	
Passwo	yrd	
Confirm Passwo	vrd	
	Cance	
Services		¢
Services NTP		
Primary NTP Server	Secondary NTP Server	
NTP Server Add	iress 192.168.1.44 NTP Server Address	
Authentication	Type None  Authentication Type None	-
	ок	Cancel

Selanjutnya kita akan melakukan konfigurasi Authentikasi Server profile untuk integrasi ke dalam AD melalui LDAP, konfigurasi melalui menu **Device**  $\rightarrow$  LDAP  $\rightarrow$  Add buatlah sesuai dengan contoh gambar di bawah ini

LDAP Server	Profile			0
Profile	Name AD-server			
	Administrator Use	e Only		
Server list	t		Server settings	
Name	LDAP Server	Port	Туре	active-directory 💌
SRV1	192.168.1.44	389	Base DN	DC=galaxidata,DC=local
			Bind DN	paload@galaxidata.local
			Password	
🕂 Add 🗧			Confirm Password	
Enter the IP ad	dress or FQDN of the LDAP server		Bind Timeout	30
			Search Timeout	30
			Retry Interval	60
				Require SSL/TLS secured connection
				Verify Server Certificate for SSL sessions
				OK Cancel

<u>paload@galaxidata.local</u> adalah username yang telah kita create sebelumnya untuk digunakan palo alto firewal dalam melakukan integrasi ke dalam AD, isikan IP server AD dan port yang digunakan dalam melakukan integrasi AD,

setelah selesai jangan lupa untuk melakukan **Commit** configuration agar konfigurasi dapat di apply ke dalam system. Untuk melihat apakah integrasi telah success silahkan lihat system log pada dashboard melalui menu **Dashboard** → **System Logs** selanjutnya kita akan melakukan testing Integrasi AD dengan mencoba testing login AD menggunakan user "**paload**" yang sebelumnya telah kita buat, lakukan testing melalui CLI interface dengan perintah

">test authentication authentication-profile AD-server username paload password"

admin@PA-VM-Galaxi> test authentication authentication-profile AD-User username paload password Enter password : Target vsys is not specified, user "paload" is assumed to be configured with a shared auth profile. Do allow list check before sending out authentication request... name "paload" is in group "all" Authentication to LDAP server at 192.168.1.44 for user "paload" Egress: 192.168.1.1 Type of authentication: plaintext Starting LDAP connection... Succeeded to create a session with LDAP server DN sent to LDAP server: CN-paload, CN-Users, DC-galaxidata, DC-local User expires in days: never

Jika success Contoh seperti gambar berikut

Jika gagal maka error akan muncul pada jendela CLI

Selanjutnya kita akan melakukan configurasi **WMI authentication** agar active directory server dapat terdiscover pada **Server Monitoring window,** lakukan konfigurasi WMI authentication melalui menu **Device** → **User Identification** → **User Mapping** → kemudian lakukan konfigurasi WMI authentication menggunakan user yang suah kita buat "paload" menggunakan format domainname\username "galaxidata\paload" dan isikan password AD user tersebut.

Palo Alto Networks User ID Agent Setup 💿												
WMI Authentication	Server Monitor	Client Probing	Cache	NTLM	Redistribution	Syslog Filters	Ignore User List					
User Name galaxidata\paload												
Password												
Co	onfirm Password 🔸	•••••										
						ОК	Cancel					

Kemudian pastikan pada server monitoring AD server sudah terdeteksi dan dalam keadaan status **Connected**, seperti gambar di bawah ini

Server Monitoring									
Enabled	Туре	Network Address	Status						
$\checkmark$	Microsoft Active Directory	server1.galaxidata.local	Connected						
	Enabled	Enabled Type ✓ Microsoft Active Directory	Enabled     Type     Network Address       Image: Server1.galaxidata.local     Server1.galaxidata.local						

sebelum kita dapat melakukan discover terhadap **user/group** yang dimiliki oleh active direktori melalui palo alto firewall lakukan konfigurasi **Group Mapping Setting** melalui menu **Device** → **User Identification** → **Group Mappinng Setting** → **Add**, kemudian lakukan konfigurasi seperti contoh gambar di bawah ini

Group Mapping	0
Name GroupAD	
Server Profile Group Include List Custom Group	
Server Profile AD-server Voltate Interval [60 - 86400]	
Domain Setting	
User Domain	
Group Objects	
Search Filter	
Object Class group	
Group Name name	
Group Member member	
User Objects	-1
Search Filter	
Object Class person	
User Name sAMAccountName	
Mail Domains	
Mail Attributes mail	
Domain List	i I
Enabled	
ок Сап	cel

Klik **OK** kemudian **Commit** dan perhatikan menu **Group Include List** apakah group Active Directori kita sudah terbaca atau tidak, contoh seperti gambar di bawah ini

Group Mapping					0
Name GroupAD					
Server Profile Group Include List	Custom Group	)			
Available Groups			Included Groups		
	<b>→</b> ×				
▼	<b>^</b>				
Image: Computer co					
Image: Computers in a controllers in		Ð			
ou=engineer ou		•			
ou=finance					
Cn=foreignsecurityprincipals					
Image: Comparison of the service accounts in the se					
Image: Comparison of Compar					
Cn=system	-				
				ок	Cancel

Jika sudah berarti palo alto sudah berhasil terintegrasi ke dalam active directory,

Selanjtnya kita harus melakukan konfigurasi **Enable User Identification** pada zone yang kita inginkan untuk dapat melakukan identifikasi user, lakukan konfigurasi melalui menu **Network → Zones**, pada contoh disini saya mempunyai zona internal dimana user akan mengakses seperti pada contoh gambar di bawah

Zone			0
Name	Internal	User Identification ACL	
	Service Profile Zone for NSX	Include List	
Туре	Layer3	Internal	
Interfaces 🔺			
ethernet1/2			
		🛨 Add 🖿 Delete	
		Users from these addresses/subnets will be identified.	
		Exclude List A	
🗛 Add 🛛 🗖 Delata		Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24	
Zone Protection Profile	None		
Log Setting	None	🕂 Add 🗖 Delete	
	Enable User Identification	Users from these addresses/subnets will not be identified.	
		OK	]

Lakukan centang pada Enable User Identification

yang terakhir adalah kita akan melakukan test **policy profile** melalui menu **Policy** → **Security** → **Add**, silahkan coba melakukan policy firewall profile dengan melakukan filtering berdasarkan username/group, pada contoh disini saya memilih filtering poliy firewall dari local menuju internet berdasarkan user ID, pada tab **User** click **Add** maka seharusnya anda sudah dapat melihat list user dan group AD sperti contoh gambar di bawah ini

Secu	rity Po	licy Rule						0		
Gen	eral	Source	User	Destination	Application	Service/URL Category	Actions			
sele	ect		~			any	~			
	Source	e User 🔺				🔲 HIP Profiles 🔺				
	galaxidata\access control assistance operators									
	galaxio	lata\adminis	trators							
	galaxic galaxic	lata\allowed lata\backup	operators	sword replication	group					
	galaxio	lata\cert pu	blishers							
	galaxio	lata\certifica	te service	dcom access						
Ð	galaxic galaxic	lata\cloneab lata\cryntog	ile domain ranhic on	controllers		🕂 Add 🖃 Delete				
	galaxid	lata\denied	rodc pass	word replication	group					
	galaxid	lata\distribu	ted com u	isers				OK Cancel		
	galaxid	lata\dnsadm	nins				\			

Selamat Mencoba

Sumber :

https://live.paloaltonetworks.com/t5/Management-Articles/Agentless-User-IDaccess-denied-Error-in-Server-Monitor/ta-p/62346

https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-Agentless-User-ID/ta-p/62122

https://live.paloaltonetworks.com/t5/Management-Articles/Palo-Alto-PAN-OS-Windows-AD-Integration-Tech-Note/ta-p/66222

https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Troubleshoot-LDAP-Authentication/ta-p/61818

https://www.youtube.com/watch?v=3DB9OZt-13s

# 15.Reset Factory Default configurasi Palo Alto (setelah berhasil Login)

Kita dapat melakukan reset configurasi setting pada palo alto firewall, namun ketika kita melakukan reset configurasi maka "settingan konfigurasi dan log pada palo alto firewall akan hilang", untuk melakukan reset konfigurasi kita dapat melalui menu command line interface dengan mengetikkan

> debug system maintenance-mode



Setelah kita pilih "y" maka system selanjutnya akan melakukan reboot dan masuk kepada maintenance mode seperti gambar di bawah ini



Press "enter" untuk melajutkan maintenance mode, setelah melakukan enter maka selanjutnya kita akan diberikan kepada beberapa pilihan menu seperti gambar di bawah ini



Selanjutnya pilih "factory reset" melalui arrow navigate keyboard untuk melakukan reset configurasi dan press enter untuk memilih menu factory reset

## 16.Reset Factory default config dan reset password administrator

Pada saat melakukan booting PAN OS press "enter" untuk melakukan stop autobooting kemudian ketik "maint" untuk masuk kepada pilihan menu maintenance seperti berikut ini

PANOS (	maint-other)	
PHNUS C	Maint) susrootA)	
THHOU (	5,51,55,65,75	
llaa	the A and I have to calcat which entry is highlighted	
Use	the $\uparrow$ and $\downarrow$ keys to select which entry is highlighted.	
Pres	s enter to boot the selected US or 'p' to enter a	
	word to unlock the next set of features	

Pilih "PANOS (Maint) untuk menggunakan menu maintenance, dan kemudian akan dibawa ke menu untuk melakukan maintenance seperti gambar di bawah ini



Press "enter" untuk melanjutkan



Pilih factory reset dan press "enter" untuk memilih menu factory reset

	Factory	Reset		
WARNING: Performing a f	actory reset will r	emove all logs	and configuration.	
Using Image: (X) panos-7.1.0				
< <u>F</u> actory Reset				>
< Advanced				$\rightarrow$
Q=Quit,	Up∕Down=Navigate,	ENTER=Select,	ESC=Back	



Silahkan tunggu proses factory reset sampai selesai seperti gambar di bawah ini

Setelah selesai silahkan lakukan reboot seperti gambar di bawah ini

	Facto	ry Reset Status		
Factory Reset Sta	utus: Success			
< Back				)
< <u>R</u> eboot				2
Bootstrapping [pa Installing pack Installing: 1 Installing: 5 Installing: 6 Installing: 6 Installing: 7 Installing: 7 Installing: 7 Installing: 6 Installing: 6	nos ] into parti ages into /mnt/swm libgcc-4.4.7-1.pan setup-2.5.58-4.pan liesystem-2.4.0-6. pasesystem-8.0-6.pa panos-release-2-2.p sermcap-5.5-1.20060 ac-guest-utilities- nash-5.1.19.6-2.pan gmt-dynamic-panos- pexpect-2.3-1.pan	tion "sysroot0" /sysroot0/ pan n an 701.1 xenstore-6.1.0-1033 7.1.0.0-39.vm	3. 11. pan	

Setelah dilakukan reboot Kemudian lakukan login default cridential palo alto yaitu User : admin Pass : admin Lakukan konfigurasi interface management dengan melihat interface management pada VM melalui perintah ">show interface management", kemudian delete IP address management default yaitu 192.168.1.1 dan ubah menjadi segmen address management network anda



admin@PA-VM# set deviceconfig system ip-address 192.168.98.50 netmask 255.255.25 5.0 default-gateway 192.168.98.1\_

Jika sudah melakukan konfigurasi ketik "commit" untuk menyetujuinya

Note : Jangan lupa untuk melakukan konfigurasi default gateway karena secara default appliance palo alto menggunakan interface management untuk mengakses service external dan update

# 17. Ipsec VPN Site to Site (Static Route)

Berikut adalah konfigurasi Site-to-Site VPN Ipsec Tunnel menggunakan static route, dengan topologi sebagai berikut

SiteA : External Address : 192.168.10.10/24 IP Tunnel.10 : 10.10.10.1/30 Internal Address : 192.168.20.1/24 SiteB: External Address : 192.168.10.50/24 IP Tunnel.11 : 10.10.10.2/30 Internal Address : 172.16.30.1/24

### **Configure L3 Interface Internal/External**

Lakukan konfigurasi melalui menu Network → Interfaces → Ethernet

#### **Configure L3 Interface External : Site A**

Interface : ethernet1/1 Type : L3 Virtual Router : Default Zone : Untrust IPV4 : 192.168.10.10 MGMT Profile : External (allow Ping)

#### Configure L3 Interface Internal : Site A

Interface : ethernet1/2 Type : L3 Virtual Router : Default Zone : Internal Ipv4 : 192.168.20.1 Mgmt Profile : Internal\_Mgmt (allow ping, ssh, https)

Ethernet VLAN Loopback Tunnel											
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual- Wire	Security Zone	Features	Comment	
ethernet1/1	Layer3	External		External_192.168.10.10	default	Untagged	none	Untrust	Ħ		
ethernet1/2	Layer3	Internal_Mgmt		IP_Int_192.168.20.1	default	Untagged	none	Internal			

#### Configure L3 Interface External : Site B

Interface : ethernet1/1 Type : L3 Virtual Router : Default Zone : External IPV4 : 192.168.10.50 MGMT Profile : External\_iface (allow Ping)

#### Configure L3 Interface Internal : Site B

Interface : ethernet1/2 Type : L3 Virtual Router : Default Zone : Internal IPV4 : 172.16.30.1 MGMT Profile : Internal\_iface (allow Ping,SSH, HTTPS)

Ethernet VLAN Loopback Tunnel											
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual- Wire	Security Zone	Features		
ethernet1/1	Layer3	External_Iface		External_192.168.10.50	default	Untagged	none	External	Ħ		
ethernet1/2	Layer3	Internal_Iface		Internal	default	Untagged	none	Internal			

### a. Create Interface Tunnel and Assign Security Zone

Create Interface tunnel melalui menu Network → Interfaces → Tunnel → Add

### **Config Interface tunnel : SiteA**

Interface : tunnel.10 Virtual Router : Default Security Zone : VPN\_Tunnel IPv4 : 10.10.10.1/30 Mgmt Profile : Mgmt\_Tunnel (allow Ping)

## Config Interface tunnel : SiteB

Interface : tunnel.11 Virtual Router : Default Security Zone : VPN-Tunnel IPv4 : 10.10.10.1/30 Mgmt Profile : Tunnel\_Mgmt (allow Ping)

Dalam static route Ipsec VPN Tunnel sehausnya tidak dibutuhkan IP address pada interface tunnel, namun di beberapa kasus kita membutuhkan monitoring status tunnel dan kita bisa memonitoringnya melalui IP address tersebut

### b. Create Static Route melalui nexthop VPN Tunnel pada Virtual Router

Create static route melalui menu Network  $\rightarrow$  Virtual Routers  $\rightarrow$  Default  $\rightarrow$  Static Route  $\rightarrow$  Add kemudian lakukan penambahan seperti contoh pada gambar berikut

Name	Inte	erfaces	Configuration	RIP	OSPF	OSPFv3	BGP
Z default	eth						0 🗖
	tun	Router Settings	IDv4 IDv6				
		Static Routes	IFV4 IFV0			_	
		Redistribution Profile	Virtual Router - Stat	tic Route - IPv4		0	1 item 🔿 🗙
		RIP	Name	Address_Tunnel			
		OSPF	Destination	172.16.30.0/24 tunnel.10			BFD No Install
		OSPFv3	Next Hop	O IP Address O Next VF	Discard 💿 None		None
		BGP	Admin Distance	10 - 240			
		Multicast	Metric	10			
			DED D 61-	No Install			
			BFD Profile	None			
					ок	Cancel	
						_	
						ſ	
							OK Cancel

### SiteA

#### SiteB

Virtual Router - defaul					0 🗆
Router Settings	ID-4 ID-6				
Static Routes	IPV4 IPV0				
Redistribution Profile	Virtual Route	r - Static Route - IPv4		0	1 item 🔿 🗙
RIP		Name Address_Tunnel			
OSPF	Dest	ination 192.168.20.0/24		BF	D No Install
OSPFv3	In	terface tunnel.11		N	bne
BGP	Admin D	stance 10 240		one	
Multicast	Admin D	Metric 10		_	
Multicast		No Install			
	BFD	Profile None		-	
			ОК	Cancel	
	🕂 Add 🗖 D	elete 🛛 🕤 Clone			
				ſ	OK Cancel

c. Setup Crypto Profiles (IKE Crypto Profile For Phase 1 and Ipsec Crypto For Phase 2

Configure IKE Crypto (Phase1) melalui menu Network → Network Profiles → IKE Crypto Pada case di sini kita menggunakan profile default

aes-128-chc	sha256	aroun19
IKE Crypto Profile		0
Name default		
DH Group	Encryption	
group2	aes-128-cbc des	
+ Add - Delete Nove Up Nove Down	🕂 Add 🗖 Delete 💽 Move Up 💽 Move Dov	m
Authentication	Timers	
🗐 sha1	Key Lifetime Hours	
🔲 shal	Key Lifetime Hours	<b>V</b>
n sha1	Key Lifetime Hours 8 Minimum lifetime =	3 mins
Add Delete Move Up Move Down	Key Lifetime Hours 8 Minimum lifetime = IKEv2 Authentication Multiple	3 mins
Add Delete Move Up Move Down	Key Lifetime Hours 8 Minimum lifetime = IKEv2 Authentication Multiple	3 mins
Add Delete Move Up Move Down	Key Lifetime Hours 8 Minimum lifetime = IKEv2 Authentication Multiple	3 mins OK Cancel

Configure Ipsec Crypto (Phase2) melalui menu Network  $\rightarrow$  Network Profiles  $\rightarrow$  Ipsec Crypto  $\rightarrow$  Add pada contoh di sini kita menggunakan profile default

TDC or Droto col	500	-	DH Crown		
IPSec Protocol	ESP	· ·	DH Group	group2	· ·
Encryption			Lifetime	Hours 1	
aes-128-cbc				Minimum lifetime = 3 mins	
3des			Enable		
			Lifesiz	MB 💌 [1 - 65535]	
				Recommended lifesize is 100MB or greater	
🕂 Add   🖃 Delete 🛛	🕤 Move Up 🛛 💽 Move Down				
Authentication					
		_			
sha1					
sha1					
sha1					
sha1	O Marcilla - O Marci Deve				
sha1					

Seperti contoh gambar di bawah ini

#### d. Configure IKE Gateway

Tahap selanjutnya Lakukan konfigurasi IKE gateway profile melalui menu **Network** → **Network Profile** → **IKE Gateway** → **Add** kemudian lakukan konfigurasi seperti berikut

### Site A

Interface : ethernet1/1 Local IP address : 192.168.10.10 Peer IP Type : Static Peer IP Address : 192.168.10.50 Auth : Pre-Shared Key Preshared Key : isikan key Local Identification : None Advanced Options IKE Crypto Profile : Default

 112		LVDP		 LVDP	AGPTS010	Mode
IKE Gatewa	Ŋ				0	auto
General	Advanced Op	otions				
	Name	IKE-Gateway-SiteA				
	Version	IKEv1 only mode			-	
	Address Type	● IPv4 ○ IPv6				
	Interface	ethernet1/1			-	
Lo	cal IP Address	External_192.168.10.10				
	Peer IP Type	Static Opynamic				
Pe	eer IP Address	192.168.10.50				
	Authentication	Pre-Shared Key O	Certificate			
P	Pre-shared Key	••••••				
Confirm P	Pre-shared Key	•••••				
Loca	l Identification	None				
Peer	r Identification	None				
				ОК	Cancel	

### SiteB

Interface : ethernet1/1 Local IP address : 192.168.10.50 Peer IP Type : Static Peer IP Address : 192.168.10.10 Auth : Pre-Shared Key Preshared Key : isikan key Local Identification : None Advanced Options IKE Crypto Profile : Default

KE Gateway         General         Advanced Options         Name         KE-Gateway-SiteB         Version         IKEV1 only mode         Address Type         IV4         IV5         Interface         ethernet1/1         Local IP Address         IP2.168.10.50         Peer IP Type         Static         Dynamic         Peer IP Address         IP2.168.10.10         Authentication         Pre-shared Key         Local Identification         None         Peer Identification         None         OK	P	LVDP III IVDP Version
General       Advanced Options         Name       IKE-Gateway-SiteB         Version       IKEv1 only mode         Address Type       IPv4         Interface       ethernet1/1         Local IP Address       External_192.168.10.50         Peer IP Type       Static         Dynamic       Peer IP Address         Peer IP Address       192.168.10.10         Authentication       Pre-Shared Key         Confirm Pre-shared Key       Certificate         Pre-shared Key       Image: Confirm Pre-shared Key         Local Identification       None         Peer Identification       None         OK       Cancel	IKE Gateway	0
Name       IKE-Gateway-SiteB         Version       IKEV1 only mode         Address       Type         Address       Type         Interface       ethernet1/1         Local IP Address       External_192.168.10.50         Peer IP Type       Static       Dynamic         Peer IP Type       Static       Dynamic         Peer IP Address       192.168.10.10       Image: Confirm Pre-shared Key         Authentication       Pre-Shared Key       Certificate         Pre-shared Key       Image: Confirm Pre-shared Key       Certificate         Peer Identification       None       Image: Confirm Pre-shared Key       Image: Confirm Pre-shared Key         Local Identification       None       Image: Confirm Pre-shared Key       Image: Confirm Pre-shared Key       Image: Confirm Pre-shared Key         Local Identification       None       Image: Confirm Pre-shared Key       Image: Confirm Pre-shared Key       Image: Confirm Pre-shared Key         Version       None       Image: Confirm Pre-shared Key       Image: Confirm Pre-	General Advanced	Dptions
Version       IKEv1 only mode         Address Type       IPv4         Interface       ethernet1/1         Local IP Address       External_192.168.10.50         Peer IP Type       Static         Dynamic         Peer IP Address       192.168.10.10         Authentication       Pre-Shared Key         Confirm Pre-shared Key       Certificate         Pre-shared Key       Image: Confirm Pre-shared Key         Local Identification       None         Peer Identification       None         OK       Cancel	Nam	E IKE-Gateway-SiteB
Address Type  IPv4 IPv6 Interface ethernet1/1 Local IP Address External_192.168.10.50 Peer IP Type  Static  Dynamic Peer IP Address 192.168.10.10 Authentication  Pre-Shared Key  Confirm Pre-shared Key  Confirm Pre-shared Key  Pre-shared Key  Confirm None Peer Identification None  OK Cancel	Versio	IKEv1 only mode
Interface ethernet1/1	Address Typ	e 🖲 IPv4 🔵 IPv6
Local IP Address External_192.168.10.50 Peer IP Type  Static  Dynamic Peer IP Address  192.168.10.10 Authentication  Pre-Shared Key  Confirm Pre-shared Key Local Identification None Peer Identification None OK Cancel	Interfac	e ethernet1/1
Peer IP Type • Static Dynamic   Peer IP Address   192.168.10.10   Authentication • Pre-Shared Key • Certificate   Pre-shared Key   Confirm Pre-shared Key   Local Identification   None   Peer Identification   None   OK	Local IP Addres	s External_192.168.10.50
Peer IP Address 192.168.10.10   Authentication Pre-Shared Key   Pre-shared Key •••••••   Confirm Pre-shared Key •••••••   Local Identification None   Peer Identification None   OK Cancel	Peer IP Typ	e 💿 Static 🔿 Dynamic
Authentication  Pre-Shared Key  Certificate Pre-shared Key Confirm Pre-shared Key Local Identification None Peer Identification None OK Cancel	Peer IP Addres	\$ 192.168.10.10
Pre-shared Key Confirm Pre-shared Key Local Identification None Peer Identification None OK Cancel	Authenticatio	n 💿 Pre-Shared Key 🔘 Certificate
Confirm Pre-shared Key Local Identification None Peer Identification None OK Cancel	Pre-shared Ke	۷
Local Identification None	Confirm Pre-shared Ke	4
Peer Identification None	Local Identificatio	None 💌
OK Cancel	Peer Identificatio	None 💌
OK Cancel		
		OK Cancel

### e. Setup Ipsec Tunnel

#### SiteA

Lakukan konfigurasi Ipsec tunnel melalui menu **Network → IPSec Tunnels → Add** Kemudian lakukan konfigurasi seperti pada gambar di bawah ini

Tunnel Interface : tunnel.10 Address type : IPv4 Type : AutoKey IKE Gateway : IKE-Gateway-SiteA Ipsec Crypto Profile : default Show Advance Options : Enable Enable Replay Protection : Enable Tunnel Monitor : Enable Destination IP : 10.10.10.2

IPSec Tunn	iel	•	
General	Proxy ID	ls l	
	Name	Tunnel_Ipsec	
Tunnel	Interface	tunnel.10 💌	
Addr	ress Type	IPv4 IPv6	
	Туре	● Auto Key 🔿 Manual Key 🔵 GlobalProtect Satellite	
IKE	Gateway	IKE-Gateway-SiteA	
IPSec Cryp	to Profile	default 💌	
		Show Advanced Options	
		Enable Replay Protection	
		Copy TOS Header	
🖂 🗹 Tunr	nel Monit	or	
Desti	ination IP	10.10.10.2	
	Profile	None	
		OK Cancel	

### SiteB

Tunnel Interface : tunnel.11 Address type : IPv4 Type : AutoKey IKE Gateway : IKE-Gateway-SiteB Ipsec Crypto Profile : default Show Advance Options : Enable Enable Replay Protection : Enable Tunnel Monitor : Enable Destination IP : 10.10.10.1

IPSec Tunnel		0
General Proxy I	Ds de la constante de la const	
Name	IpSec-Tunnel	
Tunnel Interface	tunnel.11	-
Address Type	● IPv4 ○ IPv6	
Туре	Auto Key      Manual Key      GlobalProtect Satellite	
IKE Gateway	IKE-Gateway-SiteB	•
IPSec Crypto Profile	default	-
	Show Advanced Options	
	Imable Replay Protection	
	Copy TOS Header	
Tunnel Moni	tor	
Destination IF	10.10.10.1	
Profile	None	r
	ОК Сапсе	1

### f. Create Policy to Allow Communication VPN between Site

Create policy security untuk mengizinkan kedua site dapat berkomunikasi melalui VPN Tunnel secara bolak-balik melalui menu **Policy**  $\rightarrow$  **Security**  $\rightarrow$  **Add** seperti contoh gambar di bawah

#### SiteA & Site B

	Name	Tags	Туре	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Optio
1	Trust-to-VPN	none	universal	🚧 Internal	any	any	any	200 VPN_Tunnel	any	any	🔆 application-d	Allow	none	
2	VPN-to-trust	none	universal	(22) VPN_Tunnel	any	any	any	🕅 Internal	any	any	🗶 application-d	Allow	none	

Policy Name : **Trust-to-VPN** Source Zone : Source Addr : Any User : Any Dest Zone : VPN\_Tunnel Dest Addr : Any Application : Any Action : Allow Policy Name : **VPN-to-Trust** Source Zone : VPN\_Tunnel Source Addr : Any User : Any Dest Zone : Internal Dest Addr : Any Application : Any Action : Allow

#### g. Verification

Jika ingin melihat status interface tunnel Ipsec apakah sudah UP atau belum maka kita dapat melalui menu **Network → Ipsec Tunnel** seperti gambar di bawah ini

#### SiteA



Tu	Funnel Info - Tunnel_Ipsec										0 🗆			
٩														1 item 📑 🙁
	Name	Local IP	Local Port	Peer IP	Monitor IP	Remote IP	Remote Port	Pkt Encap	Pkt Decap	Byte Encap	Byte Decap	Acquire		Protocol
	Tunnel_I	192.168.10.10	any	192.168.10.50	10.10.10.2	0.0.0/0	any	6857	6857	822840	822840	4	1	any

```
admin@PA-UM-Site1>
admin@PA-UM-Site1> ping source 192.168.20.1 host 172.16.30.1
PING 172.16.30.1 (172.16.30.1) from 192.168.20.1 : 56(84) bytes of data.
64 bytes from 172.16.30.1: icmp_seq=1 ttl=64 time=1.31 ms
64 bytes from 172.16.30.1: icmp_seq=2 ttl=64 time=2.36 ms
64 bytes from 172.16.30.1: icmp_seq=3 ttl=64 time=2.77 ms
64 bytes from 172.16.30.1: icmp_seq=4 ttl=64 time=2.45 ms
64 bytes from 172.16.30.1: icmp_seq=5 ttl=64 time=2.23 ms
^C
--- 172.16.30.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.312/2.229/2.773/0.492 ms
admin@PA-UM-Site1> _
```

SiteB

				IKE Gateway/Satellite						Tunnel Interfac	e	
Name	Status	Туре	Interface	Local IP	Peer IP	Status	In	terface	Virtual Router	Virtual System	Security Zone	Status
✓ IpSec-Tunnel	O Tunnel Info	Auto Key	ethernet1/1	External_192.168.1	192.168.10.10	O IKE Info	tur	inel.11	default (Show Rout	vsys1	VPN-Tunnel	
Tunnel Info - IpSec	Tunnel											
					1	_	1			1		1 item → 🗙
Name	Local IP	Local Port Peer	P Monitor IF	Remote IP	Remote Port	Pkt Encap	Pkt Decap	Byte Encap	Byte Decap	Acquire	TID F	rotocol
IpSec-Tunnel	192.168.10.50	any 192.1	68.10.10   10.10.10.	0.0.0/0	any	6651	6651	798120	798120	4	1 a	iny
admin@ admin@ admin@ PING 1 64 byt 64 byt 64 byt 64 byt 64 byt ^C 19 5 pack rtt mi admin@	Image       Local PP       Local PP       Local PP       Mondbor IP       Remote IP       Pate Encap       PAt Encap       Byte Encap       Byte Decap       Acquire       TD       Produced         1 psec-Tumed       192.168.10.50       any       192.168.10.50       any       192.168.10.50       any       192.168.10.50       any       6651       6651       798120       4       1       any         addmin@PA-UM-Site2>       addmin@PA-UM-Site2>       ping       source       172.16.30.1       host       192.168.20.1       1       any         admin@PA-UM-Site2>       ping       source       172.16.30.1       host       192.168.20.1       ping       any         admin@PA-UM-Site2>       ping       source       172.16.30.1       host       192.168.20.1       ping       any         admin@PA-UM-Site2>       ping       source       172.16.30.1       host       192.168.20.1       ping       any       any </td											

## 18. Failover Link Used PBF 2 ISP (Policy Based Forwarding)

Configure Interface on Interface External and Internal melalui menu **Network** → **Interfaces** 

External ISP1 : ethernet1/1 (Primary) Type : L3 Virtual Router : Default Zone : Untrust IP Address : 172.16.10.1/24 Management Profile : Untrust

External ISP2 : ethernet1/2 (Secondary) Type : L3 Virtual Router : Default Zone : Untrust IP Address : 172.16.20.1/24 Management Profile : Untrust

Internal Gateway : ethernet1/3 Type : L3 Virtual Router : Default Zone : Untrust IP Address : 10.10.10.1/24 Management Profile : Trust

Selanjutnya lakukan konfigurasi routing static untuk backup link ISP2 kepada address destination melalui menu **Network → Virtual Router → Default → Static Route** kemudian lakukan penambahan static route seperti berikut Destination : 192.168.20.0/24 Interface : ethernet1/2 Next Hop : 172.16.20.2 Metric 10

_
⇒ ×
tall

Selanjutnya adalah membuat PBF rule untuk koneksi primarys ISP dan memaksa semua traffic yang akan menuju destination server akan melalui interface external ISP1 ethernet1/1 next hop 172.16.10.2, dan akan melakukan failover secara otomatis kepada ISP2 ketika next hop ISP1 mengalami timeout dengan fature monitor dengan membypass rule PBF jika nexthop ISP1 mengalami down, dan menggunakan routing table lookup

buatlah rule PBF melalui menu Policy  $\rightarrow$  Policies Based Forwarding  $\rightarrow$  Add

Source Zone : Trust Source Address : Any Source user : Any Destination Address : Remote Server (192.168.20.0/24) Application : any Service : Any Action : Forward Eggress Interface : ethernet1/1 Next Hop : 172.16.10.2 Monitor : Check Profile : redundant

Policy Based Forwarding Rule					
General	Source	Destination/Application/Service	Forwarding		
	Name	PBF-ISP			
0	escription				
				_	
	Tags			V	
				Cancel	

Policy Based Forwarding Rule				0				
General So	urce	Destination/Applica	ation/Service	Forwarding				
Туре	Zone		🛃 Any			any	~	L
🔲 Zone 🔺			Source Ad	ldress 🔺		Source User 🔺		
Trust								
🕂 Add 🗖 De	elete		Add DI	) el ata	_	🗛 Add 🛛 🖨 Dalata		a
			Negate				_	1
						ок	Cancel	]

Policy Based Forwarding Rule			
General Source Destination/Applic	ation/Service Forwarding		
Any	🗹 Any	any 💌	
Destination Address	Applications	Service 🛋	
🔲 🔩 Remote-Server			
🕂 Add 🗖 Delete	🕂 Add 🗖 Delete	🕂 Add 🔲 Delete	
Negate			
		OK Cancel	

Policy Based Forwarding Rule					
General Source	Destination/Application/Service Forwarding				
Action	Forward				
Egress Interface	ethernet1/1				
Next Hop	172.16.10.2				
Monitor					
Profil	Redundan 💌				
	Disable this rule if nexthop/monitor ip is unreachable				
IP Addres	35				
Enforce Sym	netric Return				
Next Hop Address	; List				
🗭 Add . 🖨 Deleti					
Schedule	None				
	OK Cancel				

Profile Monitor terdapat pada menu Network ightarrow Monitor
Monitor Profile	0
Name	Redundan
Action	○ Wait Recover    ● Fail Over
Interval (sec)	3
Threshold	5
	OK Cancel

Create SNAT untuk mentranslasikan Local network ke dalam IP External Address, lakukan SNAT untuk kedua IP external ISP yang kita miliki melalui menu **Policy**  $\rightarrow$  **NAT** 

	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	SNAT-INET	none	(22) Trust	🕅 Untrust	ethernet1/1	Se Local-Network	Semote-Server	any	dynamic-ip-and-port	none
									ethernet1/1	
									ISP1-172.16.10.1	
2	SNAT-INET2	none	🕅 Trust	🕅 Untrust	ethernet1/2	Seal-Network	Semote-Server	any	dynamic-ip-and-port	none
									ethemet1/2	
									ISP2-172.16.20.1	

Tahap terakhir adalah membuat **security Policy** untuk mengijinkan local network agar dapat berkomunikasi dengan external network public, create security policy melalui menu **Policies** 

## → Security → Add Name : Trust-Untrus

Source Zone : Trust Source Address : local network (10.10.10.0/24) Dest Zone : Untrust Dest Address : Remote Server Application : Any Service : Any Action: Allow

Selanjutnya kita akan melakukan testing failover melalui host kepada remote server, dan kita akan melakukan scenario failover

### **Normal Condtion**

lhι	utapea(	ĝSRV-J	JKT:~\$	5 ping	192	2.168.	20.1			
PIN	NG 192	.168.2	20.1 (	192.10	58.2	20.1)	56(84)	bytes	of data.	
64	bytes	from	192.1	168.20	.1:	icmp_	seq=1	ttl=63	time=0.792	ms
64	bytes	from	192.1	168.20	.1:	icmp_	seq=2	ttl=63	time=1.38	ms
б4	bytes	from	192.1	168.20	.1:	icmp_	seq=3	ttl=63	time=1.01	ms
64	bytes	from	192.1	168.20	.1:	icmp_	seq=4	ttl=63	time=1.13	ms

	Start Time	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Rule	Ingress I/F	Egress I/F	Bytes	Virtual System	Clear
-	09/13 01:34:57	Trust	Untrust	10.10.10.5	192.168.20.1	3284	18	1	ping	Trust-Untrus	ethernet1/3	ethernet1/1	196	vsys1	×
	Detail				Flow 1	/1		2							
Session ID Times 10 bytem Application Protocol Security rule NAT Destination NAT Fuel OS Class Created By Syn Cookie To Host Session Control Dy Syn Cookie To Host Session To Host Session Catholic Session Cathol		okie	47 6 1 vsys1 ping 1 Trust-Untrus Trust-Trust-Untrus SNAT-INET N/A 4 False False False False False False True False False		Direction From Zone Source Destination From Port To Port From User To User State Type	c2s Trust 10.10.10.5 192.168.20.1 3284 18 unknown ACTIVE FLOW	Direction From Zoi Source Destinati From Po To Port From Us To User State Type	i 522 ne Uni 197 t 188 er uni AC FLC	rust 1:168.20.1 1:61.0.1 14 14 14 10wm ITVE ITVE IW	-					
۲	09/13 01:34:55	Trust	Untrust	10.10.10.5	192.168.20.1	3284	16	1	ping	Trust-Untrus	ethernet1/3	ethernet1/1	196	vsys1	×
•	09/13 01:34:53	Trust	Untrust	10.10.10.5	192.168.20.1	3284	14	1	ping	Trust-Untrus	ethernet1/3	ethernet1/1	196	vsys1	×
	09/13 01:34:54	Trust	Untrust	10.10.10.5	192.168.20.1	3284	15	1	ping	Trust-Untrus	ethernet1/3	ethernet1/1	196	vsys1	×
	09/13 01:34:52	Trust	Untrust	10.10.10.5	192.168.20.1	3284	13	1	ping	Trust-Untrus	ethernet1/3	ethernet1/1	196	vsys1	×
	09/13 01:34:56	Trust	Untrust	10.10.10.5	192.168.20.1	3284	17	1	ping	Trust-Untrus	ethernet1/3	ethernet1/1	196	vsys1	×

aamin@PH-Vr	auminern-omy snow por rule all														
Rule	ID Next	Rule State Hop Status	Action	Egress	IF/USYS	NextHop									
==========	=====	=========	=======	======	=========	=======================================									
============	= ====	============													
PBF-ISP	1 UP	Active	Forward	etherne	t1/1	172.16.10.2									

Failover

```
lhutapea@SRV-JKT:~$ ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=63 time=0.776 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=63 time=1.35 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 192.168.20.1: icmp_seq=4 ttl=63 time=1.11 ms
```

	Start Time	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Rule	Ingress I/F	Egress I/F	Bytes	Virtual System	Clear
	09/13 01:39:22	Trust	Untrust	10.10.10.5	192.168.20.1	3305	45	1	ping	Trust-Untrus	ethernet1/3	ethernet1/2	196	vsys1	×
11	Detail				Flow 1		Flow 2	w 2							
Session ID Trimeau Statem Virtual Statem Protocol Security Rule NAT Bule QoS Rule Created By Syn Cookie Created By Syn Cookie Created By Syn Cookie Session End Log Session End Log Session End Log Session End Log Session End Log Session Frame Ha		okie	309 voye1 1 Trust-Untus Trust-Untus SIMAT-NET2 SIMA SIMA False False False False Tust False False False False		Direction C2s From 2010 Destination 192168,20.1 From Vot 305 From User unknown To User unknown To User Inflorent State Inflorent FLOW		Direction From Zo Source Destinati From Po To Port From Us To User State Type	Direction         s2C           From Zone         Untrust 2001           From Zone         172.68.20.1           Destination         172.16.20.1           From Port         3395           To Port         3395           State         unknown           To Port         3395           State         UNIT           Type         FLOW							
	09/13 01:39:26	Trust	Untrust	10.10.10.5	192.168.20.1	3305	49	1	ping	Trust-Untrus	ethernet1/3	ethernet1/2	196	vsys1	×
	09/13 01:39:27	Trust	Untrust	10.10.10.5	192.168.20.1	3305	50	1	ping	Trust-Untrus	ethernet1/3	ethernet1/2	196	vsys1	×
	09/13 01:39:25	Trust	Untrust	10.10.10.5	192.168.20.1	3305	48	1	ping	Trust-Untrus	ethernet1/3	ethernet1/2	196	vsys1	×
	09/13 01:39:23	Trust	Untrust	10.10.10.5	192.168.20.1	3305	46	1	ping	Trust-Untrus	ethernet1/3	ethernet1/2	196	vsys1	×
	09/13 01:39:21	Trust	Untrust	10.10.10.5	192.168.20.1	3305	44	1	ping	Trust-Untrus	ethernet1/3	ethernet1/2	196	vsys1	×
	09/13 01:39:24	Trust	Untrust	10.10.10.5	192.168.20.1	3305	47	1	ping	Trust-Untrus	ethernet1/3	ethernet1/2	196	vsys1	×

System Logs	S X
Description	Time
Vsys 1 PBF rule PBF-ISP is Bypassed	09/13 01:38:29
Vsys 1 PBF rule PBF-ISP nexthop is DOWN	09/13 01:38:29



Dan dia akan kembali menggunakan ISP1 melalui rule PBF jika monitoring melihat bahwa nexthop interface ISP1 sudah normal kembali / UP

# **19.ECMP Load Balancing**

Konfigurasi ini digunakan ketika kita mempunyai 2 link internet dari ISP yang berbeda dan ingin melakukan load balance internet outbond traffic agar dapat meningkatkan performance internet access

Konfigurasi Interface :

Untuk Interface Address dan topologi, kita menggunakan topologi pada pembahasan sebelumnya yaitu pada PBF, dan yang kita lakukan kali ini hanyalah mengubah mode routing forwarding yang sebelumnya menggunakan PBF untuk redudansi traffic (Active-Passif) melalui 2 ISP yang dimiliki menjadi ECMP (Equal Cost Multipath) agar dapat menjadi (Active-Active) redundansi internet out traffic.

Sesudah melakukan konfigurasi interface selanjutnya kita akan menambahkan 2 Default route melalui 2 link ISP yang berbeda yaitu : ISP1 dan ISP2, lakukan penambahan default router melalui menu Network  $\rightarrow$  Virtual Routers  $\rightarrow$  Default  $\rightarrow$  Static Route

	IPv4	IPv6								
	٩									2 items 🔿 🗙
					Nex	t Hop				
		Name	Destination	Interface	Туре	Value	Admin Distance	Metric	BFD	No Install
L		Default-Route2	192.168.20.0/24	ethernet1/2	ip-address	172.16.20.2	default	10	None	
L		Default-route1	192.168.20.0/24	ethernet1/1	ip-address	172.16.10.1	default	10	None	
L										

Seperti yang dapat dilihat bahwa kita telah menambahkan default route melalui 2 link internet yang kita miliki yaitu melalui ISP1 dan melalui ISP2 menggunakan metric cost yang sama yaiut 10, selanjutnya untuk mengaktifkan feature ECMP gunakan menu Network  $\rightarrow$  Virtual Routers  $\rightarrow$  Default  $\rightarrow$  ECMP seperti gambar di bawah ini

General E	CMP			
	I Enable	Interface	Weight	
	Symmetric Return			
Max Path 2				
Load Balan	ice			
Method	Balanced Round Robin			
		🕂 Add 🔲 Delete		
			ОК	Cancel

Seperti pada gambar di atas kita telah mengaktifkan feature ECMP pada virtual router "default" maximum melalui 2 Link Path dan menggunakan method load balancing "balanced round robin".

Selanjutnya buat security policy dan SNAT agar internal network dapat mengakses external network (untrust) untuk koneksi internet melalui 2 link internet yang kita miliki, untuk membuat security policy gunakan menu Policies  $\rightarrow$  Security  $\rightarrow$  Add

## Name : Trust-Untrust

Source Zone : Trust Source Address : local network (10.10.10.0/24) Dest Zone : Untrust Dest Address : Remote Server Application : Any Service : Any Action: Allow

Lakukan juga konfigurasi SNAT, untuk mentranslasikan address local internal menjadi IP public interface external melalui menu Policy  $\rightarrow$  NAT

#### Name : SNAT-INET

Source Zone : Trust Destination Zone : Untrust Destination Interface : ethernet1/1 Source address : Local network (10.10.10.0/24) Destination Address : Remote Server (192.168.20.0/24) Source Translation : Dynamic-ip-and-port Address Type : Interface Address Interface : ethernet1/1 IP Address : ISP1-172.16.10.1

#### Name : SNAT-INET2

Source Zone : Trust Destination Zone : Untrust Destination Interface : ethernet1/2 Source address : Local network (10.10.10.0/24) Destination Address : Remote Server (192.168.20.0/24) Source Translation : Dynamic-ip-and-port Address Type : Interface Address Interface : ethernet1/2

								Translated Packet				
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation		
1	SNAT-INET	none	(22) Trust	(22) Untrust	ethernet1/1	Se Local-Network	Semote-Server	any	dynamic-ip-and-port	none		
									ethemet1/1			
									ISP1-172.16.10.1			
2	SNAT-INET2	none	(22) Trust	🕅 Untrust	ethernet1/2	Seal-Network	🛬 Remote-Server	any	dynamic-ip-and-port	none		
									ethernet1/2			
									ISP2-172.16.20.1			

## Testing

destination hit nh_id/mask	nexthop	flags	interface	мtu weight
192.168.20.0/24	172.16.20.2	uge	ethernet1∕2	1500 100
1122 0/1				
	172.16.10.1	uge×	ethernet1∕1	1500 100
1121 1/1				

admin@PA-VM> show routing fib virtual-router default ecmp yes\_

paloalto		Dashboard	ACC	Monit	r	Policies	Obiects	Network	Device							4	Commit 🔏 👔
							,										
V 🖬 Logs	Filt	ers										⇒ ×	÷				
R Traffic		Start Time	From	Zone Tr	Zone	Source	Dec	tination	From Port	To Port	Protocol	Application	Pula	Ingress I/F	Enress I/E	Bytec	Virtual System
Threat		00/12 21:21:47	Tout		Lone	10 10 10 5	102	169.20.1	54676	22		opplication	Touch United	athemat1/2	athemat1/2	0060	virtual System
URL Filtering		09/15 21:51:47	Trust	0	urusi	10.10.10.2	192	.100.20.1	34070	1050	0	SSII	Trust-Ontrus	etternet1/5	ethemet1/2	9000	VSYSI
WildFire Submissions		09/13 22:02:29	Trust	U	trust	10.10.10.5	192	.168.20.1	3132	1850	1	ping	Trust-Untrus	etnemet1/3	etnemet1/1	98	VSVS1
Data Hitering	-	09/13 22:02:27	Trust	U	trust	10.10.10.5	192	.168.20.1	3132	1848	1	ping	Trust-Untrus	ethernet1/3	ethemet1/1	98	vsys1
Configuration		09/13 22:02:24	Trust	U	trust	10.10.10.5	192	.168.20.1	3132	1845	1	ping	Trust-Untrus	ethernet1/3	ethernet1/2	196	vsys1
System		09/13 22:02:28	Trust	U	trust	10.10.10.5	192	.168.20.1	3132	1849	1	ping	Trust-Untrus	ethernet1/3	ethernet1/2	196	vsys1
Alarms	۲	09/13 22:02:26	Trust	U	trust	10.10.10.5	192	.168.20.1	3132	1847	1	ping	Trust-Untrus	ethernet1/3	ethernet1/2	196	vsys1
🖼 Unified	۲	09/13 22:02:25	Trust	U	trust	10.10.10.5	192	.168.20.1	3132	1846	1	ping	Trust-Untrus	ethernet1/3	ethernet1/1	98	vsys1
P Packet Capture																	
V 🖓 App Scope																	
Summary																	
Change Monitor																	
Threat Monitor																	
😡 Threat Map																	
Metwork Monitor																	
Carrier Resures	1																
Session Browser																	

Pada skenario di sini saya melakukan PING dan SSH access kepada remote internal address palo alto, dan dapat dilihat pada **Monitor**  $\rightarrow$  **Session Browser** bahwa egress interface di load balancing untuk setiap traffic/new session kepada ISP1 dan ISP2,

Note : Ketika salah satu link Ex : ISP1 mengalami down maka traffic akan secara otomatis akan diarahkan kepada link internet ISP2 ketika kita memulai session yang baru, dan selama internet link ISP1 dalam keadaan down, paket akan tetap diarahkan kepada ISP1 yang mengalami down, kemudian selanjutnya ke ISP2

# 20. High Availability (Acive – Passive)

Pada sesi kali ini kta akan melakukan konfigurasi HA pada palo alto firewall appliance, mode HA pada palo alto ada 2 yaitu active-active / active-pasive, namun pada kesempatan ini saya akan melakukan konfigurasi active-passive.

Untuk melakukan konfigurasi HA pada palo alto terdapat beberapa kebutuhan yang harus kita miliki agar kedua appliance dapat bergabung sebagai HA configuration,

 Pada appliance yang memiliki port dedicated HA pada appliance gunakan ethernet cable crossover jika kedua appliance direct connected satu dengan yang lain, jika appliance tidak memiliki dedicated port HA gunakan dua port data pada appliance untuk kita jadikan sebagai interface mode HA.

Untuk pembentukan HA sendiri dibutuhkan 3 Port yang digunakan dalam konfigurasi HA yaitu

- HA1(Controll link)  $\rightarrow$  dapat menggunakan interface management
- HA1(Backup)  $\rightarrow$  dapat menggunakan port dedicated HA atau port data yang sudah di setting sebagai interface HA
- HA2 (Data Link) → Dapat menggunakan port dedicated HA atau port data yang sudah di setting sebagai interface HA
- 2. Pastikan NTP sudah tersinkronisasi

Konfigurasi :

a. Apabila kita menggunakan interface management sebagai HA1 kita harus memastikan bahwa interface management dapat di reach satu dengan yang lainya melalui Ping, untuk itu pastikan interface management sudah mengaktifkan feature allowed ping melalui menu Device → Setup → Management → Management Interface Setting

	Hostname PA-V/M									
Management Interface Settings										
ІР Туре	Static O DHCP Client	Services								
IP Address	192.168.98.50	П НТТР	Permitted IP Addresses							
Netmask	255.255.255.0	HTTP OCSP								
Default Gateway	192.168.98.1	HTTPS								
IPv6 Address/Prefix Length		Telnet								
Default IPv6 Gateway		SSH SSH								
Speed	auto-negotiate 💌	V Ping								
MTU	1500	SNMP								
		User-ID								

b. Jika appliance tidak memiliki dedicated HA port kita dapat merubah data port menjadi interface HA melalui menu Network → Interfaces → Ethernet pilih interface dan pada interface type ubah menjadi type HA seperti gambar di bawah

Ethernet Interface	0
Interface Name	ethernet1/1
Comment	
Interface Type	HA
Advanced	
Link Settings	
Link Speed au	to Link Duplex auto Link State auto
	OK Cancel

Lakukan hal di atas untuk interface selanjutnya pada port data yang akan kita jadikan menjadi interface HA

c. Konfig HA mode dan Group ID melalui menu Device → High Availability → General
 → Edit dan lakukan konfigurasi seperti gambar di bawah ini

Setup	Ø
	Enable HA
Group ID	10
Description	
Mode	Active Passive      Active Active
	Enable Config Sync
Peer HA1 IP Address	
Backup Peer HA1 IP Address	
	OK Cancel

Group ID adalah unik indentifikasi yang digunakan untuk mengidentifikasi sebuah group HA, lakukan konfigurasi yang sama pada peer HA dengan Group ID yang sama juga, gunakan mode **Active-Passive** 

d. Lakukan konfigurasi HA interface untuk HA1 (controller Link) menggunakan intetrface management, lakukan konfigurasi pada menu Device → High Availability
 → General dan edit Controll link (HA1) Section, dan konfigurasi seperti gambar di bawah ini

Control Link (HA1)	0
Port	management
	C Encryption Enabled
Monitor Hold Time (ms)	3000
	OK Cancel

Pada controller link kita akan menggunakan interface management

e. Enable encryption pada controller link dengan melakukan export haKey dari salah satu appliance dan mengimport key tersebut kepada peer HA lainya, lakukan export haKey melalui salah satu appliance pada menu Device → Certificate Management → Certificates → Export HA Key kemudian simpan key tersebut kepada local drive anda.

Selanjutnya lakukan **login kepada peer HA** appliance masuk kepada menu **Device**  $\rightarrow$  **Certificate Management**  $\rightarrow$  **Certificates**  $\rightarrow$  **Import HA key** lalu import haKey file yang sudah kita simpan dalam local drive untuk di import kepada appliance tersebut

Terakhir yaitu kita akan mengaktifkan checkbox "Encryption Enabled" pada control link dengan mencentang option tersebut pada settingan **Device**  $\rightarrow$  **High Availability**  $\rightarrow$  **General** seperti gambar di atas

f. Lakukan konfigurasi pada interface HA1 backup (control link) melalui menu Device
 → High Availability → General edit contol link HA1 Backup section menjadi seperti gambar di bawah ini

192.168.98.51	
Control Link (HA1 B	ackup) 💿
Port	ethemet1/1
IPv4/IPv6 Address	20.20.20.1
Netmask	255.255.255
Gateway	
	OK Cancel

Control Link (HA1 Backup)										
Port	ethernet1/1									
IPv4/IPv6 Address	20.20.20.2									
Netmask	255.255.255.0									
Gateway										
	OK Cancel									

Karena kita menggunakan port data yang dijadikan sebagai port HA maka kita harus memberikan alamat address kepada port tersebut agar HA peer dapat berkomunikasi satu dengan yang lainya melalui link tersebut, **apabila peer conection masih dalam satu network kita tidak perlu memberikan default gateway pada settingan address** untuk interface tersebut

g. Lakukan konfigurasi Data Link (HA2) melalui menu Device → High Availabilit → General edit section Data link (HA2) dan pilih interface/port yang akan digunakan sebagai data link pada HA seperti contoh gambar di bawah

Data Link (HA2)	0									
Enable Session Synchronization										
Port	ethernet1/2									
IPv4/IPv6 Address										
Netmask										
Gateway										
Transport	ethernet 💌									
🚽 🗹 HA2 Keep-ali	ve									
Actio	on 💿 Log Only 🔿 Split Datapath									
Threshold (ms	s) 10000									
	OK Cancel									

Karena kita menggunakan transport secara default dia akan memilih ethernet sebagai media komunikasi dan akan saling terkoneksi jika interface tersebut dikoneksikan kepada peer HA baik direct atau melalui switch, jika komunikasi kepada peer membutuhkan route maka kita bisa menggunakan menggunakan IP sebagai transport mode, dan pastikan centang checbox "Enable Session Synchronization" seperti gambar di atas

 h. Enable HA Heartbeat Backup jika anda menggunakan port Data sebagai control link HA melalui menu Device → High Availabbility → Election Setting seperti gambar di bawah ini

2	Election Settings
	Device Priority 255
	V Preemptive
	🗹 Heartbeat Backup
v	HA Timer Settings Recommended
	OK Cancel

Namun jika menggunakan interface management sebagai control link hal ini tidak perlu dilakukan

 Lakukan konfigurasi device priority pada kedua HA appliance, semakin rendah nominal priority maka dia akan semakin prefer sebagai active firewall HA dan pastikan checkbox preemptive sudah enable seperti contoh gambar di bawah ini

2	Election Settings
	Device Priority 100
	V Preemptive
l	Heartbeat Backup
v	HA Timer Settings Recommended
	OK Cancel

j. Lakukan konfigurasi akhir untuk mengaktifkan feature HA untuk melakukan sinkronisasi configurasi dan redudansi jika salah satu appliance mengalami error, gunakan menu Device → High Availability → Setup edit section setup menjadi seperti gambar di bawah

Setup		0
	🗹 Enable HA	
Group ID	10	
Description		
Mode	Active Passive      Active Active	- 6
	Enable Config Sync	- 1
Peer HA1 IP Address	192.168.98.51	
Backup Peer HA1 IP Address	20.20.20.2	
	OK Cancel	

Setup	0
	🗹 Enable HA
Group ID	10
Description	
Mode	Active Passive      Active Active
	🗹 Enable Config Sync
Peer HA1 IP Address	192.168.98.50
Backup Peer HA1 IP Address	20.20.20.1
	OK Cancel

Checkbox "enable HA" dan "enable config sync" dan masukkan link HA1 peer IP address dan backup HA1 peer address seperti gambar di atas

k. Apabila semua konfigurasi sudah dilakukan, selanjutnya adalah melakukan verifikasi apakah HA konfigurasi berhasil atau tidak diimplementasikan kepada kedua appliance palo alto, lakukan ferifikasi dengan menambahkan widget High Availibilty pada dashboard melalui menu Dashboard → Widget → System seperti gambar di bawah ini

	Dashboard	ACC		Monitor		Polic	ies	Objects	s Netw	ork	Device			
	Layout: 3 Columns	~	88	Widgets 👻			d: <b>15:31</b> :1	12						
				Application	•	S ×	Logged	In Admins	5				5.1	Config Log
ame	PA-VM			System			Admin	Fr	om		Client	Session Start	Idle For	Comman
ress	192.168.98.50			Logs	•		admin	19	2.168.98.32		Web	09/13 23:09:18	00:00:00s	commit
ıask	255.255.255.0													set
way	192.168.98.1						Data Lo	gs					S 1	٠
ress	unknown						No data	available.						Locks
ress	fe80::20c:29ff:fea1:c005/6	54												LUCKS No looks (
way							High Av	ailability					S 1	
ress	00:0c:29:a1:c0:05								Mode		Active-nassive			ACC Dick
odel	PA-VM								Local	0	Passive			AGC NISK I
al #	unknown							Peer (1	92.168.98.51)	ă	Active			No data fo
J ID	E3060500FFFBAB1F							R	unning Config	ŏ	Synchronized	2		
UID	564D5F18-DBC0-CA27-E20	DD-2E136	DA1C	005					App Version	ŏ	Match			
inse	none							1	Threat Version	ŏ	Match			
ode	VMWare ESXi							Ant	tivirus Version	ŏ	Match			
sion	7.1.0							PA	AN-OS Version	ŏ	Match			
lent	0.0.0							GlobalP	rotect Version	ŏ	Match			
sion	564-3168								HA1	ŏ	Up			
sion	0000.00.00.000	_							HA1 Backup	õ	Up			
ime	Thu Sep 14 01:31:53 2017	7							HA2	õ	Up			
ime	0 days, 4:27:02										-			

Periksa status running config synchronisasi apabila belum tersinkron lakukan sinkronisasi dengan mengklik status running config "**sycn to peer**", jika HA barhasil maka pada widget maka kita akan melihat status widget seperti berikut ini

#### Active

General Information		S ×	Logged In A	dmins				S ×
General Information Device Name MGT IP Address MGT Default Gateway MGT IPv6 Default Gateway MGT IPv6 Link Local Address MGT IPv6 Default Gateway MGT IPv6 Default Gateway MGT MAC Address MOdel Serial # CPU ID UUID	PA-VM-Site2 192.168.98.51 255.255.255.0 192.168.98.1 unknown fe80:20c:29ff:fe8c:ce75/64 00:0c:29:8c:ce:75 PA-VM unknown E3060500FFFBAB1F 564D72FE-391F-F22E-EBC2-7362288CCE75	S X	Logged In A Admin admin Data Logs No data avai High Availat	dmins From 192.168.98.249 lable. bility Mode Local eer (192.168.98.50) Running Config Ann Version	Client Web Active-passive Active Passive Synchronized Match	Session Start 09/14 14:42:11	Idle Fo 00:00:00	S X bs
VM License VM Mode Software Version GlobalProtect Agent Application Version URL Filtering Version Time Uptime	none VMWare ESXi 7.1.0 0.0.0 564-3168 0000.00.00.000 Thu Sep 14 15:34:48 2017 0 days, 1:08:10		G	App Version Threat Version Antivirus Version PAN-OS Version IobalProtect Version HA1 HA1 Backup HA2	Match Match Match Match Up Up			

#### Passive

General Information	S X	Logged In A	dmins					S ×
Device Name	PA-VM	Admin	From		Client	Session Start	Idle For	
MGT IP Address	192.168.98.50	admin	192.168.98.32		Web	09/13 23:09:18	00:00:00s	
MGT Netmask	255.255.255.0							
MGT Default Gateway	192.168.98.1	Data Logs						😋 🛛
MGT IPv6 Address	unknown	No data avai	lable.					
MGT IPv6 Link Local Address	fe80::20c:29ff:fea1:c005/64							
MGT IPv6 Default Gateway		High Availab	oility					S ×
MGT MAC Address	00:0c:29:a1:c0:05		Mada		Activo passiv			
Model	PA-VM		Mode	•	Acuve-passiv	e		
Serial #	unknown		LUCdi	2	Assive			
CPU ID	E3060500FFFBAB1F	P	Durating Config	~	Acuve	. B.		
UUID	564D5F18-DBC0-CA27-E20D-2E136DA1C005		Ann Version	~	Synchronized			
VM License	none		App Version	~	Match			
VM Mode	VMWare ESXi		Anticiana Mansian		Match			
Software Version	7.1.0		Antivirus Version		Match			
GlobalProtect Agent	0.0.0		PAN-US Version		Match			
Application Version	564-3168	G	Inderstore version	~	match			
URL Filtering Version	0000.00.000		HA1	~	Up			
Time	Thu Sep 14 01:31:53 2017		HAI BACKUP	~	Up			
Uptime	0 days, 4:27:02		HAZ	0	Up			

Pada Active HA interface port selain yang digunakan oleh HA akan tetap active(UP) namun pada passive, selain interface yang digunakan untuk komunikasi HA akan mengalami state down, dan interface tersebut akan active jika Active HA mengalami down dan melakukan failover kepada HA passive

A	С	t	İ١	V	e
A	С	t	ľ	V	e

Ethernet VLAN Loo	pback Tunnel									
a										
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual- Wire	Security Zone	Features	Comment
ethernet1/1	HA			none	none	Untagged	none	none		
ethernet1/2	HA			none	none	Untagged	none	none		
ethernet1/3	Layer3	Trust		none	default	Untagged	none	Trust		
ethernet1/4			m	none	none	Untagged	none	none		
ethernet1/5			m	none	none	Untagged	none	none		
🚥 ethernet1/6			Ē	none	none	Untagged	none	none		

### Passive

I	Ethernet VLAN Loopback Tunnel								
	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual- Wire	Security Zone
	ethernet1/1	HA			none	none	Untagged	none	none
	ethernet1/2	HA			none	none	Untagged	none	none
	ethernet1/3	Layer3	Trust		none	default	Untagged	none	Trust
	ethernet1/3	Layer3	Trust		none	default	Untagged	none	Trust