

Installation Steps for Virtual Wire Mode Evaluation

Thank you for choosing to evaluate a Palo Alto Networks firewall. The steps below explain how to install and configure the firewall in your network. Feel free to call your Sales Engineer for assistance during your installation and evaluation.

Preparation steps

- Determine where in the network you will be inserting the Palo Alto Networks device. One common location is between the gateway firewall and the internal switch. In virtual wire mode, the Palo Alto Networks device acts as a "bump on the wire", so there is no need to re-address your network.
- Determine what IP address you'll be assigning to the firewall's management port. This IP will need Internet access to download the latest OS and licenses.

Part 1: Configuring the Management Port

1. Power on the Palo Alto Networks firewall. Connect via the console cable (9600-8-N-1). Login using the defaults:

Username: **admin** Password: **admin**

2. You will receive a message that the system is initializing. It may take a few minutes for the device to initialize. You can monitor the status of the startup using the CLI command **show jobs processed**. When the output of that command shows a status of FIN, the device has completed its boot sequence.

admin@PA-2020> show jobs processed Type Status Result Completed Enqueued ID 02:52:14 1 AutoCom ACT PEND 50% admin@PA-2020> admin@PA-2020> show jobs processed Type Status Result Completed Enaueued ID. OK 02:53:20 02:52:14 1 AutoCom FIN

Do not proceed until the device has completely initialized.

3. You will now configure the management interface of the Palo Alto Networks firewall. Fill in the following information:

Mgmt interface IP:	_
Mgmt interface mask:	_
Mgmt interface gateway:	
Mgmt interface DNS server:	

4. From the console, execute the commands below. Make sure to replace the variables with the information you recorded in the previous step.

```
configure
set deviceconfig system ip-address x.x.x.x netmask y.y.y.y default-gateway z.z.z.z dns-primary v.v.v.v
commit
exit
```

Here is an example of these commands.

```
admin@PA-4020> configure

Entering configuration mode

[edit]

admin@PA-4020# set deviceconfig system ip-address 1.1.1.12 netmask 255.255.255.0

default-gateway 1.1.1.254 dns-primary 4.2.2.2

[edit]

admin@PA-4020# commit

.....10%.....20%.....30%.....40%.....50%.....60%.....70%.....80%.....

90%.....100%

Configuration committed successfully

[edit]

admin@PA-4020#
```

- 5. Attach the firewall's management port to your network. The management port must be cabled to a switch port that is set to **auto-detect all settings**.
- 6. To test connectivity, ping from the firewall to a device on your network, for example, ping to your default gateway (z.z.z.z)

```
ping host z.z.z.z
```

Press control-C to end the pings. Here is an example:

PANOS 3.0.0

```
admin@PA-2020> ping host 1.1.1.254

PING 1.1.1.254 (1.1.1.254) 56(84) bytes of data.

64 bytes from 1.1.1.254: icmp_seq=1 ttl=64 time=2.98 ms

64 bytes from 1.1.1.254: icmp_seq=2 ttl=64 time=1.44 ms

64 bytes from 1.1.1.254: icmp_seq=3 ttl=64 time=1.41 ms

64 bytes from 1.1.1.254: icmp_seq=4 ttl=64 time=1.51 ms

64 bytes from 1.1.1.254: icmp_seq=5 ttl=64 time=1.45 ms

64 bytes from 1.1.1.254: icmp_seq=6 ttl=64 time=1.47 ms

--- 1.1.1.254 ping statistics ---

6 packets transmitted, 6 received, 0% packet loss, time 4999ms

rtt min/avg/max/mdev = 1.413/1.714/2.982/0.567 ms
```

You should test network connectivity to the DNS server, as well as to the Internet. (Note that the firewall must have Internet access so that it can download licenses and the latest OS.) Do not proceed until you have the proper connectivity.

Part 2: Installing Licenses and Updating Software

7. You will use the web user interface of the firewall to for the remainder of the configuration. On the management workstation, open a browser to the IP address of your management interface. Make sure to use SSL to connect to the firewall (https://) You will see a certificate warning—that is ok, continue to the web page. You will be prompted with a login screen. Login to the firewall with the same username and password as via the console.



8. Once logged in, the home screen will appear. You will use the tabs across the top, and the menus in the left column, to configure the device.

Note: If you have connectivity problems with the UI, make sure that the switch port that is physically cabled to the management port is set to "auto".

- 9. Configure a more secure administrator password using **Device** -> **Administrators**. Make sure to write down this new password.
- 10. You must register your product in order to download your eval licenses. Go to <u>https://support.paloaltonetworks.com</u>. In the bottom left corner, click **Register**. Enter in the appropriate information to create a login account. Also enter your serial number on that page. You can find your device's serial number in the bottom right corner of the initial firewall logon page.

General Information	×
Device Name	PA-4020
IP Address	1.1.1.12
Netmask	255.255.255.0
Default Gateway	1.1.1.254
MAC Address	00:30:48:60:39:fe
Model	PA-4020
 Serial #	0002A100212
Software version	3.0.0
SSL-VPN Client	0.0.0
Application version	117-78
Threat version	0
URL Filtering version	
Time	Sun Jun 28 14:11:29 2009
Uptime	0 days, 0:04:10

- 11. To set the time and date of your device, go to the **Device** tab -> **Setup** menu. In the right column, towards the bottom, click on **Set Time**. Enter an accurate date and time.
- 12. While still on the Device -> Setup screen, in the left column at the top, click on **Edit**. On this screen you can do the following:
 - Change the timezone.
 - Enter the NTP server information.
 - Configure the services that you want the MGT interface to respond to.

	- MCT Interface Services											
FIGI IN	terrace Serv	ices										
НТТР 📃	HTTPS 🔽	Telnet 📃	SSH 🔽	Ping 🔽	SNMP 🔽							

• Under Geo Location, enter the latitude and longitude of your location. This will place the graphic for your firewall in the proper location on the world map. The example below is appropriate for San Diego, CA:

Geo Loca	tion
Latitude	32
	(-90.0 to 90.0)
Longitude	-117
	(-180.0 to 180.0)

13. Now you will download your licenses from the license server. Since you entered both a default gateway and DNS server IP address via the console, the firewall will be able to download the licenses via the management port. On the tabs across the top, select **Device**. On the menu on the left, select **Licenses**. The screen below will appear.

NETWORKS	Dashboard	ACC	Monitor	Policies	Objects	Network	Device
							0
Device	License	s					
- Admin Roles	Licens	e Management			-		
-S Administrators	Retrie	ve license keys	from license serve	r			
User Identification	Activa	ite feature usini	g authorization cod	le			
High Availability	Manua	ally upload licen	se key				
Certificates							
Response Pages							
E-U Log Settings							
- System							
Contig							
Log Destinations							
- I SIMP Irap							
- Empl							
Child							
leare							
- Oscis							
Authentication Profile							
- Scheduled Log Export							
- On Software							
-02 SSL-VPN Client							
Dupamic Undates							
- Q Licenses							
Ca Support							

- 14. Select **Retrieve license keys from license server**. Assuming the firewall can reach the Palo Alto Networks license server on the Internet, the licenses will be downloaded and installed for the features that you requested to evaluate.
- 15. At this point, you will commit your config. In the top-right corner of the browser window, click on **Commit**. This configuration will be saved to the firewall's hard drive as well as to the running config.



16. Next, you will make sure you are running the appropriate version of PANOS. Go the Device tab -> Software menu. You will see the following:

Software					
Version	Size	Release Date	Downloaded	Currently Installed	Action
Error: No up	odate info	ormation available			

17. On the bottom of the screen, click on the **Refresh** button. The list of the latest versions of PANOS will be retrieved. Your screen will be similar to the one shown here:

Softwar	Software Last updated at: 07/21 02:55:11									
Version	Size	Release Date	Downloaded	Currently Installed	Action					
3.0.0	158 MB	2009/06/16 03:25:44			Download	Release Notes				
2.1.6	101 MB	2009/07/09 10:38:07	~	~	Install	Release Notes	×			
2.1.5	101 MB	2009/05/29 16:04:41			Download	Release Notes				
2.1.4	103 MB	2009/04/22 21:03:58			Download	Release Notes				

18. Select the version of PANOS software that your SE recommends you install, and click **Download**.

Note that PANOS 3.0.0 requires that the device be running 2.1.5 or higher. If the device is NOT at 2.1.5+ and you try to download PANOS 3.0.0, you will get a cryptic error message.

Softwa	re				Last	updated at: 07/2	1 02:55:11
Version	Size	Release Date	Downloaded	Currently Installed	Action		
3.0.0	158 MB	2009/06/16 03:25:44			Download	Release Notes	
2.1.6	101 MB	2009/07/09 10:38:07	~	~	Install	Release Notes	×
2.1.5	101 MB	2009/05/29 16:04:41			Download	Release Notes	
2.1.4	103 MB	2009/04/22 21:03:58			Download	Release Notes	

19. Once downloaded, you will see the screen below.

S	h	tν	v:	ar	0
9					-

Last updated at: 07/21 02:55:11

Version	Size	Release Date	Downloaded	Currently Installed	Action		
3.0.0	158 MB	2009/06/16 03:25:44	~		Install	Release Notes	×
2.1.6	101 MB	2009/07/09 10:38:07	~	~	Install	Release Notes	×
2.1.5	101 MB	2009/05/29 16:04:41			Download	Release Notes	

- 20. Click **Install** to upgrade your device. Reboot your device when prompted. After the device reboots, login to the web user interface.
- 21. You will download the latest URL filtering and threat databases. Go to Device tab -> Dynamic Updates. Click on the button Check Now. You will see an updated list of the latest Application and Threats database, and the latest URL Filtering database. Your screen will look similar to the one below.

									_
Applicatio	on and Threats								
Version	Feature	Туре	Size	Release Date	Downloaded	Installed	Action		
129-196, 129	9-196 Apps, Threats	Full	124 MB	2009/06/24 11:34:34		(Download	Release Notes	
Check No	W Last checked:	2009/06/2	28 14:20:5	5 Schedule: Every w	ednesday at 01:02 (download-only)	Upload	Install from	File
Check No	w Last checked:	2009/06/2	28 14:20:5	5 Schedule: Every w	ednesday at 01:02 (idownload-only)	Upload	Install from	File
Check No URL Filteri Version	w Last checked: ing Currently Installe	2009/06/2 ed	28 14:20:5 Acti	5 Schedule: Every w	ednesday at 01:02 (idownload-only)	Upload	Install from	File
URL Filteri Version	w Last checked: ing Currently Installe	2009/06/2 ed	28 14:20:5	5 Schedule: Every w	ednesday at 01:02 (download-only)	Upload	Install from	File

- 22. **Download** the latest Application and Threats database, and then **Install** it. (You can view the download and installation status using the CLI command **show jobs processed**.)
- 23. Configure the Application and Threat database to be automatically downloaded and installed. Next to the word Schedule, click on the blue text "Every Wednesday at 01:02 (download-only)".

Dynamic Update	S						
Application and	Threats						
Version	Feature	Туре	Size	Release Date	Downloaded	Currently Installed	Action
129-196, 129-196	Apps, Threats	Full	124 MB	2009/06/24 11:34:34	Ý	Ý	
Check Now L	ast checked: 2	009/06/28	3 14:37:43	Schedule: Every wed	nesday at 01:02 (do	wnload-only) Upl	oad

24. A popup will appear. Configure the update schedule to be on a daily basis, at a time that you select, and configure the database to be both downloaded and installed automatically.

Recurrence	Daily 💌
Time	3 💙 : 30 🗸
Action	Download and install

25. Commit your changes.

26. Go to the **Device** tab -> **Licenses** page. Examine the URL Filtering portion. The Brightcloud URL database should have been automatically downloaded, and the screen should match the following:

URL Filtering		
Date Issued	June 25, 2009	
Date Expires	June 20, 2010	
Description	BrightCloud URL Filtering	
Active	No	Activate

If the URL database is still downloading, you will see the percent complete.

If you do NOT see the word "Activate", and the database is not currently downloading, you should initiate the download of the database using this command:

request url-filtering upgrade brightcloud

Wait a few minutes for the database to be downloaded. Refresh the licenses page, and the word "Activate" should appear.

- 27. Click Activate to activate the Brightcloud database. The system will reboot.
- 28. It will take a few minutes for the device to boot to an operational status. Once you login to the GUI, go to **Device** tab -> **Licenses** page to confirm that the BrightCloud database is now active.

URL Filtering					
Date Issued	June 25,	2009			
Date Expires	June 20,	2010			
Description	BrightClo	BrightCloud URL Filtering			
Active	~				
Download Status	Jun 28 14 was down	4:27:47 Initial Brightcloud URL database nloaded successfully			

Part 3: Configuring Virtual Wire Mode

The factory default configuration places $e^{1/1}$ and $e^{1/2}$ into a "virtual wire", which is what is used in vwire mode.

29. Go to Network tab -> Interfaces. A list of the interfaces will appear, as shown below.

Inte	erfaces								
	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
	ethernet1/1	VWire					Untagged	default-vwire	untrust
	ethernet1/2	VWire		111			Untagged	default-vwire	trust
Δ	ethernet1/3						Untagged		none
Δ	ethernet1/4			1			Untagged		none
Δ	ethernet1/5			1			Untagged		none
Δ	ethernet1/6			1			Untagged		none

If you want to use interfaces other than e1/1 and e1/2, delete those two from default-vwire, and put the other two interfaces into the default-vwire. Go to **Network** tab -> **Virtual Wire** to do this.

Virtua	al Wires			
	Name	Interface1	Interface2	
	default-vwire	ethernet1/1	ethernet1/2	

30. Go to the **Policies** tab. Confirm there is a rule from trust to untrust that permits all traffic.

Se	curity	Rules							
	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action
1	rule 1	1922 trust	🚧 untrust	any	any	any	any	any	0

31. If you have inbound connections, create a new rule to allow that inbound traffic, as shown here:

Security Rules

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action
1	rule1	🕅 trust	🚧 untrust	any	any	any	any	any	0
2	rule2	622	622 August	anv	anv	anv	anv	anv	

32. Commit your configuration.

Part 4: Putting the Device Inline

- 33. During a maintenance window, physically cable e1/1 to your untrusted network, and e1/2 to your trusted network.
- 34. Generate traffic from your trusted network to your untrusted network. Confirm that the traffic is going through the firewall device successfully.
- 35. Go to **Monitor** tab -> **Logs** -> **Traffic**. You will see completed sessions listed there.
- 36. If you created a policy from untrust to trust, test generating traffic in that direction as well.
- 37. After fifteen minutes or so, the firewall will begin to display graphs and tables under the Dashboard and ACC tabs. You can use those two tabs, as well as Monitor, to learn about the traffic that is traversing your network.
- 38. Confirm that all applications are traversing the firewall as expected. If there is a particular application that is not working, you may need to disable TCP SYN checking. The Palo Alto firewall, by default, will drop all data for sessions where it did not see the initial connection setup (TCP SYN packets). When the firewall was inserted in the network, there may have been existing sessions that were not able to re-establish. To disable TCP SYN checking, use these CLI commands:

```
configure
set deviceconfig setting session tcp-reject-non-syn no
commit
show session info
```

The output of show session info will tell you if the setting is "yes" or "no"

After a few hours, you can re-enable syn checking, and the application should work fine.

Part 5: Implementing Security Profiles

Now that you are satisfied that traffic is traversing the firewall, you can implement security profiles. Security profiles will inspect permitted traffic for viruses and threats, and perform URL filtering.

39. Go to Objects tab -> Security Profiles -> Antivirus. Create a New profile called "alert all viruses". Configure alerting on all of the decoder protocols. Enable packet capture as well.

Anti-Virus Virus Exception						
Packet Capture						
Decoders						
Decoder	Action					
All	Select 💙					
ftp	alert 💌					
http	alert 💌					
imap	alert 💌					
pop3	alert 💌					
smb	alert 💌					
smtp	alert 💌					

40. Go to **Objects** tab -> **Security Profiles** -> **Anti-spyware**. Create a **New** profile called "alert all spyware". Configure alerting for adware/spyware downloads via all of the decoder protocols. Enable packet capture.

Download Protection	Phone Home P	rotection Spyware	Exce
Packet Capture	~		
Decoders			
Decoder	Adware	Spyware	
All	alert 💌	alert 💌	
ftp	alert 🗸	alert 💌	
http	alert 🗸	alert 💌	
imap	alert 💌	alert 💌	
рор3	alert 💌	alert 💌	
smb	alert 🗸	alert 💌	
smtp	alert 💌	alert 💙	

Select the **Phone Home Protection** tab. This monitors for spyware trying to communicate with its central controlling machine. Enable alerts on all critical, high, and medium severity events. Also enable packet capture.

Download Pro	tection Phone Home Protection
Type Rules	Simple 💌
Severity	Actions
Critical	alert 💌
High	alert 😽
Medium	alert 💌
Low	default 💌
Informational	default 💌
Packet Captu	re 🔽

41. Go to **Objects** tab -> **Security Profiles** -> **Vulnerability Protection**. Create a **New** profile called "alert all crit-high-med vuln". Configure alerting for critical, high and medium severity attacks on a client, as well as on a server. Enable packet capture.

Name	alert all crit-high-med vuln					
Description						
Vulnerability	Vulnerabilit	y Exception				
Rule Type	Simple	*				
Rules Client			Server			
Severity	Actions		Severity	Actions		
Critical	alert 💌		Critical	alert 🗸		
High	alert 🗸		High	alert 💌		
Medium	alert 🗸	_	Medium	alert 🗸 🗸		
Low	default 🗸		Low	default 💌		
Informational	default 🐱	_	Informational	default 💌		
Packet Captu	ire 🗹					

42. Go to the **Objects** tab -> **Security Profiles** -> **URL filtering**. The default profile will be shown. Create a **New** profile called "alert all URL". In the top right corner, specify action of **alert** for all categories.

Category	Action
Set for all categories	alert 💌
abortion	alert 🗸
abused-drugs	alert 🗸
adult-and-pornography	alert 🗸

43. You will now enable inspection of permitted traffic for the threats you specified in the different security profiles. Go to the **Policies** tab. On the rule from trust to untrust, in the Profile column, click on the word **None**. Select the security profiles that you created.

Profile Groups		
Group	None 😪 New	
💿 💿 Individual Profile	s	
Antivirus Profile	alert all viruses 💌	New
Vulnerability Protection Profile	alert all crit-high-med vuln 🗸	New
Anti-Spyware Profile	alert all spyware 💙	New
URL Filtering Profile	alert all URL 💌	New
File Blocking Profile	None 💌	New
Data Filtering Profile	None 💌	New

44. Your policy should now show icons in the Profile column, like this:

Application	Service	Action		Profile		Options
any	any	0	3	0	0	

- 45. If you have a policy from untrust to trust, enable the same security profiles on that rule as well.
- 46. Commit the changes to your device.
- 47. Best practice: save your configuration to a named configuration file, and export that file to the local PC. To do this, go to the **Device** tab -> **Setup**, and in the right-hand column, select **Save named config snapshot**.

Configuration Management	
Validate candidate config	
Save candidate config	
Revert to running config	
Revert to last saved config	
Save named config snapshot	
Load named config snapshot	
Load config version	
Export named config snapshot	
Export config version	
Import named config snapshot	
Name backup_062809	
Enter a name or select one,	

Now, export that config to the local PC.



Configuration backup 062809 🗸	
Select the configuration you want to export.	
	OK Cancel

You can go back to this configuration at a later time by performing:

- 1. Import named config snapshot
- 2. Load named config snapshot

You can now test the threat detection features of the firewall as you see fit.