High Availability Synchronization

PAN-OS 5.0.3

Revision B

Contents

Overview

Palo Alto Networks high availability (HA) provides customers with robust networking and security functionality by providing continuous operations in two HA modes: Active-Passive and Active-Active. Each HA mode has its benefits and understanding how configuration parameters and system runtime information is synchronized between HA members will allow you to configure and tune the firewall's HA configuration more effectively. It is important to note that each version of PAN-OS can vary in how configuration and system runtime information is synchronized between high availability pair members – as new features can be added, existing features may be enhanced, and outdated features removed.

The following high availability architecture was used to document the synchronization outcomes discussed in this document:

Firewall devices:	PA-2020
OS Version:	PAN-OS v5.0.3
HA mode:	Active-Passive and Active-Active

Although configuration changes can be made on either HA member, our lab testing made all configuration changes on the Active (A/P) or Active-Primary (A/A) member and synchronized them with the corresponding HA peer. There are some cases where configuration changes must be made on both devices in the HA pair. Examples of these occurrences include:

- Installing and enabling licenses for specific feature sets such as Virtual Systems or URL Filtering.
- Configuring the IP addresses on the interfaces that were synchronized from the Active-Primary to the Active-Secondary member in an Active-Active deployment.

Recommendation: Configuration changes should only be made on one HA member at a time. When configuration changes are made, a "commit" is required to activate the changes into the running configuration. It is important to note that only one commit can be active at any given time. Using Commit Locks to prevent simultaneous changes in a multi-administrator environment can help prevent confusion where one administrator's changes are overwritten by another administrator's changes.

As a best practice, always try to avoid making changes on both HA members and committing changes at the same time. Allow the commit to complete on the Active (A/P) or Active-Primary (A/A) device and synchronize the changes to its peer before making further changes and committing them – don't overlap commit and synchronization tasks.

This document will concentrate on how configuration changes are synchronized in both Active-Passive and Active-Active deployments so customers can gain a better understanding of when configurations must be made on the HA peer device in addition to the primary device. The document breaks down the configuration changes into several groupings to match the PAN-OS configuration tabs in the web interface.

- Device
- Network
- Objects
- Policies
- Other

Note: The configuration synchronization matrix in each section will show the HA deployment mode as "A/P" for Active-Passive and "A/A" for Active-Active. Active-Active testing was performed with the Virtual Router and QoS synchronization options enabled.

Device Configuration

The device configuration synchronization matrix illustrates which configuration changes are synchronized between the HA members in each of the high availability modes, Active-Passive and Active-Active, for the Device Tab components.

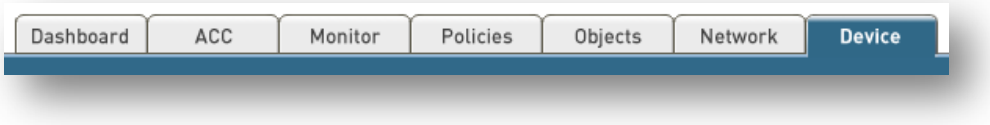
DEVICE TAB	Config Synched?		Comments
	A/P	A/A	
Setup > Management			
General Settings			
Hostname	No	No	
Domain	No	No	
Login Banner	No	No	
Time Zone	No	No	
Locale	No	No	
Date	No	No	
Time	No	No	
Latitude	No	No	
Longitude	No	No	
Auto Acquire Commit Lock	Yes	Yes	
Certificate Expiration Check	Yes	Yes	
Multi Virtual Systems Capability	No	No	Need separate license to activate. Activation will suspend peer until setting matches. Commit required.
Authentication Settings			
Authentication Profile	No	No	
Certification Profile	No	No	
Idle Timeout	Yes	Yes	
Failed Attempts	Yes	Yes	
Lockout Time	Yes	Yes	
Logging and Reporting Settings			
Log Storage	Yes	Yes	
Max Rows in User Activity Report	Yes	Yes	
Max Rows in CSV Export	Yes	Yes	
Number of Versions for Config Audit	Yes	Yes	
Average Browse Time	Yes	Yes	
Page Load Threshold	Yes	Yes	
Send Hostname in Syslog	Yes	Yes	
Stop Traffic when LogDB Full	Yes	Yes	

DEVICE TAB	Config Synched? A/P	Config Synched? A/A	Comments
Enable Log on High DP Load	Yes	Yes	
Panorama Settings			
Panorama Servers	No	No	
Receive Timeout for Connection	Yes	Yes	
Send Timeout for Connection	Yes	Yes	
Retry Count for SSL Send	Yes	Yes	
Panorama Policy & Objects	No	No	
Device and Network Template	No	No	
Management Interface Settings			
IP Address	No	No	
Network Mask	No	No	
Default Gateway	No	No	
IPv6 Address/Prefix Length	No	No	
Default IPv6 Gateway	No	No	
Speed	No	No	
MTU	No	No	
Services	No	No	
Permitted Addresses	No	No	
Minimum Password Complexity			
Password Format Requirements	Yes	Yes	
Functionality Requirements	Yes	Yes	
Setup > Operations			
Miscellaneous			
Custom Logos	Yes	Yes	
SNMP Setup	No	No	
Statistics Service	No	No	
Setup > Services			
Services			
DNS Servers	No	No	
DNS Proxy Object	No	No	
Primary/Secondary DNS Server	No	No	
Primary/Secondary NTP Server	No	No	
Update Server	No	No	
Proxy Server	No	No	
Service Route Configuration	No	No	

	Config Synched?	

DEVICE TAB	A/P	A/A	Comments
Service Features			
Service Route Configuration	No	No	
Setup > Content-ID			
URL Filtering			
Dynamic URL Cache Timeout	Yes	Yes	
URL Continue Timeout	Yes	Yes	
URL Admin Override Timeout	Yes	Yes	
URL Admin Lockout Timeout	Yes	Yes	
X-Forwarded-For	Yes	Yes	
Strip X-Forwarded-For	Yes	Yes	
Allow Forwarding of Decrypted Content	Yes	Yes	
URL Admin Override	Yes	Yes	
Content-ID Features			
Manage Data Protection	No	No	
Container Pages	Yes	Yes	
Settings > Wildfire			
General Settings			
Wildfire Server	Yes	Yes	
Maximum File Size	Yes	Yes	
Session Information Settings			
Source IP	Yes	Yes	
Source Port	Yes	Yes	
Destination IP	Yes	Yes	
Destination Port	Yes	Yes	
Virtual System	Yes	Yes	
Application	Yes	Yes	
User	Yes	Yes	
URL	Yes	Yes	
Filename	Yes	Yes	
Setup > Session			
Session Settings			
Rematch Sessions	Yes	Yes	
ICMPv6 Token Bucket Size	Yes	Yes	
ICMPv6 Error Packet Rate	Yes	Yes	
IPv6 Firewall	Yes	Yes	
NAT64 IPv6 Minimum MTU	Yes	Yes	
Accelerated Aging	Yes	Yes	

DEVICE TAB	Config Synched?		Comments
	A/P	A/A	
Accelerated Aging Threshold	Yes	Yes	
Accelerated Aging Scaling Factor	Yes	Yes	
Session Features			
Decryption Certificate Revocation Settings	Yes	Yes	
Session Timeouts			
Default	Yes	Yes	
Discard Default	Yes	Yes	
Discard TCP	Yes	Yes	
Discard UDP	Yes	Yes	
ICMP	Yes	Yes	
Scan	Yes	Yes	
TCP	Yes	Yes	
TCP Handshake	Yes	Yes	
TCP Init	Yes	Yes	
TCP Wait	Yes	Yes	
UDP	Yes	Yes	
Captive Portal	Yes	Yes	



Device Tab left hand side menu components:

DEVICE TAB	Config Synched?		Comments
	A/P	A/A	
Config Audit	No	No	Not Applicable
Admin Roles	Yes	Yes	
Password Profiles	Yes	Yes	
Administrators	Yes	Yes	
Virtual Systems	Yes	Yes	
Shared Gateways	Yes	Yes	
User Identification			
User Mapping	Yes	Yes	
Server Monitoring	Yes	Yes	
Include/Exclude Networks	Yes	Yes	
User-ID Agents	Yes	Yes	
Terminal Services Agents	Yes	Yes	
Group Mapping Settings	Yes	Yes	

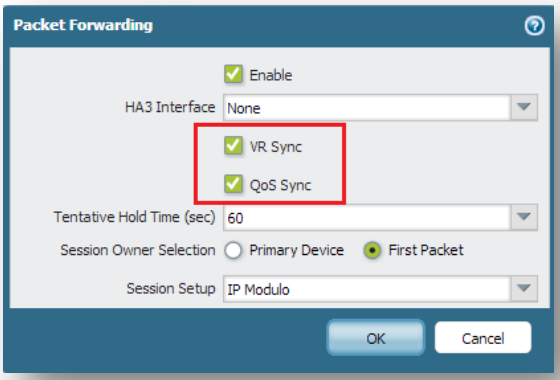
DEVICE TAB	Config Synched? A/P	Config Synched? A/A	Comments
Captive Portal Settings	Yes	Yes	Redirect address is not synchronized in A/A unless virtual/floating IP is configured
High Availability			
General Setup	No	No	
Active/Passive Settings	No	N/A	Only for A/P configurations
Election Settings	No	No	
Control Link (HA1)	No	No	
Control Link (HA1 Backup)	No	No	
Control Link (HA2)	No	No	
Control Link (HA2 Backup)	No	No	
Link and Path Monitoring			
Link Monitoring	No	No	
Link Group	No	No	
Path Monitoring	No	No	
Path Group	No	No	
Active/Active Config			
Packet Forwarding	N/A	No	Only for A/A configurations
Virtual Address	N/A	Yes	Only for A/A configurations
Operational Commands	No	No	Not Applicable
Certificate Management			
Certificates			
Device Certificates	Yes	Yes	
Default Trusted Certificate Authorities	Yes	Yes	
Certificate Profile	Yes	Yes	
OSCSP Responder	Yes	Yes	
Response Pages	Yes	Yes	

DEVICE TAB	Config Synched?		Comments
	A/P	A/A	
Log Settings			
System	Yes	Yes	
Config	Yes	Yes	
HIP Match	Yes	Yes	
Alarms	Yes	Yes	
Manage Logs	No	No	Not Applicable
Server Profiles			
SNMP Trap	Yes	Yes	
Syslog	Yes	Yes	
Email	Yes	Yes	
Netflow	Yes	Yes	
RADIUS	Yes	Yes	
LDAP	Yes	Yes	
Kerberos	Yes	Yes	
Local User Database			
Users	Yes	Yes	
User Groups	Yes	Yes	
Authentication Profile	Yes	Yes	
Authentication Sequence	Yes	Yes	
Scheduled Log Export	No	No	
Software	No	No	Synch optional, separate activation
Global Protect Client	No	No	Synch optional, separate activation
Dynamic Updates	No	No	Synch optional
Licenses	No	No	Must enter separately for each FW
Support	No	No	
Master Key and Diagnostics	No	No	Must be same value on both members, requires manual entry on each device. Disable "Config Sync" in HA Setup before changing the Master Key. Once Master Key is changed on both devices, re-enable "Config Sync" option for HA Setup.

Network Configuration

The network configuration synchronization matrix illustrates which configuration changes are synchronized between the HA members in each of the high availability modes, Active-Passive and Active-Active, for the Network Tab components.

Note: Active-Active testing was performed with the Virtual Router and QoS synching options enabled. To set these settings, go to the Device > High Availability > Active/Active Config tab and select the options to synchronize.

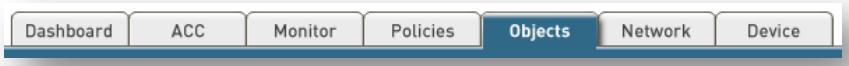


Note: VR Sync should not be used if dynamic routing protocols are used.

NETWORK TAB	Config Synched? A/P	A/A	Comments
Interfaces			
Ethernet	Yes	Yes	L2 Interfaces not supported in A/A IP addresses not synched in A/A
VLAN	Yes	Yes	L2 VLANs not supported in A/A L3 VLANs are supported in A/A
Loopback	Yes	Yes	IP addresses not synched in A/A
Tunnel	Yes	Yes	IP addresses not synched in A/A
Zones	Yes	Yes	
VLANs	Yes	Yes	IP addresses not synched in A/A
Virtual Wires	Yes	Yes	
Virtual Routers	Yes	Yes	A/A depends if VR Synchronization is enabled
IPSec Tunnels	Yes	No/Yes*	* A/A depends on virtual IP (floating IP) configuration
DHCP Server	Yes	Yes	
DHCP Relay	Yes	Yes	
DNS Proxy	Yes	Yes	
Global Protect			
Portals	Yes	No/Yes*	* A/A depends on virtual IP (floating IP) configuration
Gateways	Yes	No/Yes*	* A/A depends on virtual IP (floating IP) configuration
QOS	Yes	Yes	A/A depends if QoS Synchronization is enabled
Network Profiles			
IKE Gateways	Yes	No/Yes*	* A/A depends on virtual IP (floating IP) configuration
IPSec Crypto	Yes	Yes	
IKE Crypto	Yes	Yes	
Monitor	Yes	Yes	
Interface Mgmt	Yes	Yes	
Zone Protection	Yes	Yes	
QoS Profile	Yes	Yes	

Objects Configuration

The network configuration synchronization matrix illustrates which configuration changes are synchronized between the HA members in each of the high availability modes, Active-Passive and Active-Active, for the Objects Tab components.



OBJECTS TAB	Config Synched? A/P	Config Synched? A/A	Comments
Addresses	Yes	Yes	
Address Groups	Yes	Yes	
Regions	Yes	Yes	
Applications	Yes	Yes	
Application Groups	Yes	Yes	
Application Filters	Yes	Yes	
Services	Yes	Yes	
Service Groups	Yes	Yes	
Global Protect			
HIP Objects	Yes	Yes	
HIP Profiles	Yes	Yes	
Custom URL Category	Yes	Yes	
Dynamic Block Lists	Yes	Yes	
Custom Signatures			
Data Patterns	Yes	Yes	
Spyware	Yes	Yes	
Vulnerability	Yes	Yes	
Security Profiles			
Antivirus	Yes	Yes	
Anti Spyware	Yes	Yes	
Vulnerability Protection	Yes	Yes	
URL Filtering	Yes	Yes	
File Blocking	Yes	Yes	
Data Filtering	Yes	Yes	
DoS Protection	Yes	Yes	
Security Profile Groups	Yes	Yes	
Log Forwarding	Yes	Yes	
Decryption Profile	Yes	Yes	
Schedules	Yes	Yes	

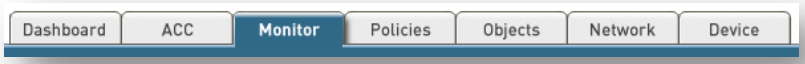
Policies Configuration

The policies configuration synchronization matrix illustrates which configuration changes are synchronized between the HA members in each of the high availability modes, Active-Passive and Active-Active, for the Policies Tab components.

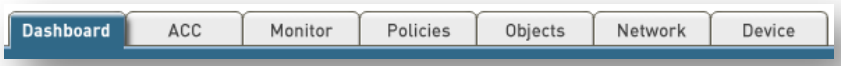
POLICIES TAB	Config Synched? A/P	Config Synched? A/A	Comments
Security	Yes	Yes	
NAT	Yes	Yes	
QoS	Yes	Yes	
Policy Based Forwarding	Yes	Yes	
Decryption	Yes	Yes	
Application Override	Yes	Yes	
Captive Portal	Yes	Yes	Redirect address is not synchronized in A/A unless virtual/floating IP is configured
DoS Protection	Yes	Yes	

Other Configurations

The other configuration synchronization matrix illustrates which configuration changes are synchronized between the HA members in each of the high availability modes in the remaining "configurable" items of the Monitor and Dashboard tabs.



MONITOR TAB	Config Synched? A/P	Config Synched? A/A	Comments
Logs	No	No	
Packet Capture	No	No	
App Scope	No	No	
Session Browser	No	No	
Botnet	No	No	
PDF Reports			
Manage PDF Summary	Yes	Yes	
User Activity Report	Yes	Yes	
Report Groups	Yes	Yes	
Email Scheduler	Yes	Yes	
Manage Custom Reports	Yes	Yes	
Reports	No	No	



	Config Synched?	

DASHBOARD TAB	A/P	A/A	Comments
Column Display	No	No	
Widgets	No	No	

Synchronizing System Runtime Information

In addition to configuration information, firewalls configured in high availability mode will also synchronize other system runtime information – such as forwarding tables, URL filtering cache tables, User-ID tables, and much more.

RUNTIME INFORMATION	Synchronized? A/P	Synchronized? A/A	HA Link	Comments
Management Plane				
User-Group Mapping	Yes	Yes	HA1	
DHCP Lease (as server)	Yes	Yes	HA1	
DNS Cache	Yes	Yes	HA1	
IPSec Keys (phase 2)	Yes	Yes	HA1	
BrightCloud URL Database	No	No		PAN-DB doesn't use a local URL database
BrightCloud URL Cache (url-filtering-feature)	No	No		Feature disabled by default, must be enabled separately on each HA member
BrightCloud Bloom Filter (url-filtering-feature)	No	No		Feature disabled by default, must be enabled separately on each HA member
PAN-DB URL Cache	Yes	No	HA1	Synchronized with DB backup to disk – every 8 hours, when URL DB version updates, or when device reboots
Content (manual sync)	Yes	Yes	HA1	
PPPoE, PPPoE Lease	Yes	Yes	HA1	
DHCP Client Settings and Lease	Yes	Yes	HA1	
SSL VPN Logged In User List	Yes	Yes	HA1	
Forward Information Base (FIB)	Yes	Yes	HA1	A/A requires VR Sync to be enabled
Data Plane				
Session Table	Yes	Yes	HA2	A/P doesn't sync ICMP A/A doesn't sync ICMP, host sessions, and multicast sessions
ARP Table	Yes	No	HA2	
Neighbor Discovery (ND) Table	Yes	No	HA2	
MAC Table	Yes	No	HA2	
IPSec Sequence # (anti-replay)	Yes	Yes	HA2	
DoS Protection	Yes	Yes	HA2	Temporary block entries for time based blocking
User-IP Mappings	Yes	Yes	HA2	User-ID Agents connection is not synched to peer. Only primary device maintains the connection to User-ID agents. Secondary will establish the connection when it is promoted to primary status.
Virtual MAC	Yes	Yes	HA2	

High Availability Link Failure

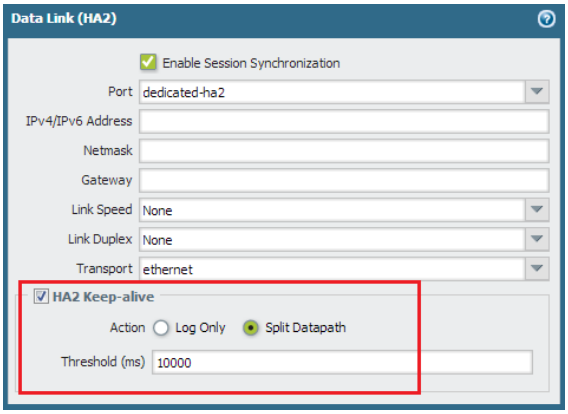
Palo Alto Networks firewalls use HA Links to synchronize information and to send session and session state information between HA pair members. Depending on the firewall model, dedicated HA interfaces may or may not be available. If

dedicated HA interfaces are available, best practice is to use these ports for the primary HA links and to configure HA Backup links to help prevent configuration mismatches, synchronization loss, and split brain conditions.

HA1 Link Failure
If the HA1 Link fails and there is no HA1 Backup configured, configuration synchronization will fail and a split brain condition will be created. Split brain conditions occur when HA members can no longer communicate with each other to exchange HA monitoring information. Each HA member will assume the other member is in a non-functional state and take over as the Active (A/P) or Active-Primary (A/A). Split brain conditions can be prevented by configuring an HA1 Backup link and/or enabling Heartbeat Backup.

HA2 Link Failure
If the HA2 Link fails and there is no HA2 Backup configured, HA members will not synchronize session and state information. Any runtime information that is normally synchronized over the HA2 link will stop synchronizing. In A/P deployments, no state transition will take place. In A/A deployments with the HA2 Keep-Alive option set to "Split Datapath", a split data path condition will be enforced and session setup and session ownership will revert back to the receiving device. Asymmetric Layer7 sessions will also be black-holed.

The HA2 Keep-alive is used to determine the health of the HA2 functionality between the HA members. It is turned off by default and if enabled, keep-alive messages will be used to determine the condition of the HA2 connection. If there is a failure of the HA2 connection(s), the HA2 Keep-alive recovery action will be taken. There are two action choices: Log Action and Split Data Path.



- **Log Action** – Logs the failure of the HA2 interface in the system log as a critical event. This action should be taken for A/P deployments as the Active HA device is the only device forwarding traffic. The Passive device is in a backup state and is not forwarding traffic, so a Split Data Path is not required. The system log will contain critical warnings indicating HA2 is down. If no HA2 Backup links are configured, state synchronization will be turned off.

05/08 10:14:06	ha	critical	ha2-keep-alive		HA Group 63: Peer HA2 keep-alive down
05/08 10:14:02	ha	critical	ha2-keep-alive		HA Group 63: All HA2 keep-alives are down; turning off state-synchronization
05/08 10:14:02	ha	critical	ha2-keep-alive		HA Group 63: Local HA2 keep-alive down
05/08 10:13:51	ha	high	ha2-link-change		HA2 peer link down
05/08 10:13:51	ha	critical	ha2-link-change		All HA2 links down
05/08 10:13:51	ha	critical	ha2-link-change		HA2 link down

- **Split Data Path** – Used in A/A deployments to instruct each HA device to take ownership of their local state and session tables. As HA2 is lost, no state and session synchronization is being performed, so a Split Data Path action is used to allow separate management of the session tables to ensure successful traffic forwarding by each HA member.

In order to prevent this condition, configure an HA2 Backup link.

HA3 Link Failure
If the HA3 Link fails, the Active-Secondary member in an A/A deployment will transition to the non-functional state. A/P deployments are not affected by an HA3 failure as HA3 is not used. To prevent this condition, configure a Link Aggregate Group (LAG) interface with two or more physical interfaces as the HA3 Link. A/A deployments do not support an HA3 Backup link. An aggregate interface with multiple interfaces will provide additional capacity and link redundancy to support packet forwarding between HA pair members.

Summary

The configuration and system runtime information synchronized between high availability members will differ depending on the HA deployment mode, version of PAN-OS, and other configuration options. Understanding these differences will help you configure the Palo Alto Networks firewalls more effectively. Configuration changes, commits, and synchronization between HA members should be planned and overlapping changes and commits should be avoided whenever possible.

Revision History

Date	Revision	Comment
May 17, 2013	B	Updated the Management Plane table and added the BrightCloud URL Database and BrightCloud URL Filter options.