Cyberoam
Unified Threat Management

High Availability Configuration Guide

Version 10

Document version 10.01.0270-1.0-05/09/2010

IMPORTANT NOTICE

Elitecore has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Elitecore assumes no responsibility for any errors that may appear in this document. Elitecore reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER'S LICENSE

The Appliance described in this document is furnished under the terms of Elitecore's End User license agreement. Please read these terms and conditions carefully before using the Appliance. By using this Appliance, you agree to be bound by the terms and conditions of this license. If you do not agree with the terms of this license, promptly return the unused Appliance and manual (with proof of payment) to the place of purchase for a full refund.

LIMITED WARRANTY

Software: Elitecore warrants for a period of ninety (90) days from the date of shipment from Elitecore: (1) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (2) the Software substantially conforms to its published specifications except for the foregoing, the software is provided AS IS. This limited warranty extends only to the customer as the original licenses. Customers exclusive remedy and the entire liability of Elitecore and its suppliers under this warranty will be, at Elitecore or its service center's option, repair, replacement, or refund of the software if reported (or, upon, request, returned) to the party supplying the software to the customer. In no event does Elitecore warrant that the Software is error free, or that the customer will be able to operate the software without problems or interruptions. Elitecore hereby declares that the anti virus and anti spam modules are powered by Kaspersky Labs and by Commtouch respectively and the performance thereof is under warranty provided by Kaspersky Labs and by Commtouch. It is specified that Kaspersky Lab does not warrant that the Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

Hardware: Elitecore warrants that the Hardware portion of the Elitecore Products excluding power supplies, fans and electrical components will be free from material defects in workmanship and materials for a period of One (1) year. Elitecore's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. The replacement Hardware need not be new or of an identical make, model or part; Elitecore may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned product that Elitecore reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware.

DISCLAIMER OF WARRANTY

Except as specified in this warranty, all expressed or implied conditions, representations, and warranties including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, non-infringement or arising from a course of dealing, usage, or trade practice, and hereby excluded to the extent allowed by applicable law.
In no event will Elitecore or its supplier be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages however caused and regardless of the theory of liability arising out of the use of or inability to use the product even if Elitecore or its suppliers have been advised of the possibility of such damages. In no event shall Elitecore's or its supplier's liability to the customer, whether in contract, tort (including negligence) or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above stated warranty fails of its essential purpose.
In no event shall Elitecore or its supplier be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

RESTRICTED RIGHTS

CORPORATE HEADQUARTERS

Elitecore Technologies Ltd.
904 Silicon Tower,
Off. C.G. Road,
Ahmedabad – 380015, INDIA
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com , www.cyberoam.com

Contents

Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office
eLitecore Technologies Ltd.
904, Silicon Tower
Off C.G. Road
Ahmedabad 380015
Gujarat, India.
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-26400707
Email: support@cyberoam.com
Web site: www.cyberoam.com

Visit www.cyberoam.com for the regional and latest contact information.

Typographic Conventions

Material in this manual is presented in text, screen displays, or command-line notation.

Item	Convention	Example
Server		Machine where Cyberoam Software - Server component is installed
Client		Machine where Cyberoam Software - Client component is installed
User		The end user
Username		Username uniquely identifies the user of the system
Part titles	Bold and shaded font typefaces	Report
Topic titles	Shaded font typefaces	Introduction
Subtitles	Bold & Black typefaces	Notation conventions
Navigation link	Bold typeface	**Group Management → Groups → Create** it means, to open the required page click on Group management then on Groups and finally click Create tab
Name of a particular parameter / field / command button text	Lowercase italic type	Enter policy name, replace policy name with the specific name of a policy Or Click Name to select where Name denotes command button text which is to be clicked
Cross references	Hyperlink in different color	refer to Customizing User database Clicking on the link will open the particular topic
Notes & points to remember	Bold typeface between the black borders	**Note**
Prerequisites	Bold typefaces between the black borders	Prerequisite Prerequisite details

Overview

Welcome to Cyberoam's – HA Configuration Guide.

Cyberoam Unified Threat Management appliances offer identity-based comprehensive security to organizations against blended threats - worms, viruses, malware, data loss, identity theft; threats over applications viz. Instant Messengers; threats over secure protocols viz. HTTPS; and more. They also offer wireless security (WLAN) and 3G wireless broadband and analog modem support can be used as either Active or Backup WAN connection for business continuity.

Cyberoam integrates features like stateful inspection firewall, VPN, Gateway Anti-Virus and Anti-Spyware, Gateway Anti-Spam, Intrusion Prevention System, Content & Application Filtering, Data Leakage Prevention, IM Management and Control, Layer 7 visibility, Bandwidth Management, Multiple Link Management, Comprehensive Reporting over a single platform.

Cyberoam has enhanced security by adding an 8th layer (User Identity) to the protocol stack. Advanced inspection provides L8 user-identity and L7 application detail in classifying traffic, enabling Administrators to apply access and bandwidth policies far beyond the controls that traditional UTMs support. It thus offers security to organizations across layer 2 - layer 8, without compromising productivity and connectivity.

Cyberoam UTM appliances accelerate unified security by enabling single-point control of all its security features through a Web 2.0-based GUI. An extensible architecture and an 'IPv6 Ready' Gold logo provide Cyberoam the readiness to deliver on future security requirements.

Cyberoam provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection.

Default Web Admin Console username is 'cyberoam' and password is 'cyber'

Cyberoam recommends that you change the default password immediately after installation to avoid unauthorized access.

Cyberoam HA

Hardware failure such as a failure of the power supply, hard disk, or processor is the main reason behind the failure of Internet security system and/or a firewall. To provide reliable and continuous connection to the Internet and also to provide security services such as firewall, VPN, Intrusion detection and prevention, virus scanning, web filtering, and spam filtering services, Cyberoam allows configuring two appliances to function as a single Cyberoam Appliance and provide high availability.

High availability solution provides efficient, continuous access to critical applications, information, and services. High availability is critical to maintaining network protection from an attack, even in the event of a device failure.

Cyberoam uses clustering technology to ensure the high availability. In a cluster, two Cyberoam Appliances are grouped together and instructed to work as a single entity.

Cyberoam HA terminology

1. HA Cluster

Group of two Cyberoam appliances instructed to work as a single entity. Every HA Cluster has one Primary Appliance and one Auxiliary Appliance. The Primary Appliance controls how the cluster operates. The roles that the primary and auxiliary appliances play in the cluster depend on the configuration mode.

2. HA Configuration Modes

Standalone

The default operation mode and means HA is not configured on the Cyberoam Appliance.

Active-Active

A configuration of HA cluster which consists of a primary unit and one auxiliary unit. In this mode, both primary unit and auxiliary unit process traffic while primary unit is in charge of balancing the traffic. Decision of load balancing is taken by the primary unit. Auxiliary unit can take over in case of a primary unit failure.

Active-Passive

A configuration of HA cluster which consists of a primary appliance and an auxiliary appliance. In this mode, only the primary appliance processes traffic while auxiliary appliance remains in stand-by mode, ready to take over if a primary appliance failure occurs.

3. Primary Appliance

The primary appliance also tracks the status of all cluster appliances. In an active-active cluster, the primary appliance receives entire network traffic and acts as the load balancer to redirect traffic to auxiliary appliance. In an active-passive cluster, the primary appliance processes the network traffic while auxiliary appliance does not process any traffic but remains in a ready to take over if primary appliance fails.

4. Auxiliary Appliance

Auxiliary Appliance is always waiting to become the primary appliance.

In an active-active cluster, Auxiliary appliance processes network traffic assigned to it by the primary appliance. In case primary appliance fails, auxiliary unit will become the primary appliance. In an active-passive cluster, Auxiliary Appliance does not process network traffic and is in stand-by and becomes active only when primary is not available to process the traffic.

5. Dedicated HA Link Port

A direct physical link between the appliances participating in HA cluster.

6. Load Balancing

An ability of HA cluster of balancing the traffic between nodes in the HA cluster.

7. Monitored Interface

Set of interfaces that are selected to be monitored. Each appliance monitors its own such interface and if any of them is goes down, appliance will remove itself from the cluster and failover will occur.

8. Virtual MAC

It is a MAC address associated with the HA cluster. This address is sent as response when any of the machines make ARP request to HA cluster. It is not the actual MAC address and is not assigned to any interface of any unit in the cluster.

A primary appliance owns the MAC address and is used for routing network traffic. All external clients' use this address to communicate with the HA cluster. In case of failover, new primary appliance will have the same MAC address as the failed primary appliance. The cluster appliance which has a Virtual MAC address acts as a Primary Appliance.

9. Primary state

In Active-Active mode, the appliance that is in charge of receiving all the traffic and load balancing is called to be in "Primary" state. An appliance can be in "Primary" state only when the other appliance is in "Auxiliary" state.

In Active-Passive mode, the appliance in charge of processing all the traffic is called to be in the "Primary" state. An appliance can be in "Primary" state only when the other appliance is in "Auxiliary" state.

10. Auxiliary state

In Active-Active mode, the appliance that receives the traffic to be processed by it from the primary appliance is called to be in "Auxiliary" state. A appliance can be in "Auxiliary" state only when the other appliance is in "Primary" state

In Active-Passive mode, the appliance which is not processing the traffic is called to be in "Auxiliary" state. An appliance can be in "Auxiliary" state only when the other appliance is in "Primary" state.

11. Standalone state

An appliance is called to be in Standalone state when it can still process network traffic and when the other appliance is not in position to process network traffic (i.e. in "Fault" state or shut down).

12. Fault state

An appliance will be in fault state when it cannot process network traffic because of a device or link failure.

13. Peer

Once the HA cluster is configured, cluster appliances are termed as Peers i.e. for Primary appliance, Auxiliary appliance is its peer appliance and vice versa.

14. Synchronization

The process of sharing the various cluster configuration between Cluster appliances (HA peers). Reports generated by Cyberoam are not synchronized.

15. Device Failover

If appliance does not receive any communication within the predetermined period of time from the HA peer, the peer appliance is considered to have failed. This process is termed as Device Failover as when this occurs, the peer appliance is taken over.

16. Link Failover

Both the appliance in an HA cluster continuously monitor the dedicated HA link and the interfaces configured to be monitored. If any of them fails it is called link failure.

17. Session Failover

Whether it is a device or link failover, session failover occurs for forwarded TCP traffic except for virus scanned sessions that are in progress, VPN sessions, UDP, ICMP, multicast, and broadcast sessions and Proxy traffic.

Cyberoam normally maintains session information for TCP traffic which is not passing through proxy service. Hence, in case of failover, the appliance which takes over will take care for all the session (TCP session not passing though proxy application) the entire process will be transparent for the end users.

How Cluster works

Cyberoam offers high availability by using Virtual MAC address shared between a primary appliance and an Auxiliary appliance linked together as a “cluster”.

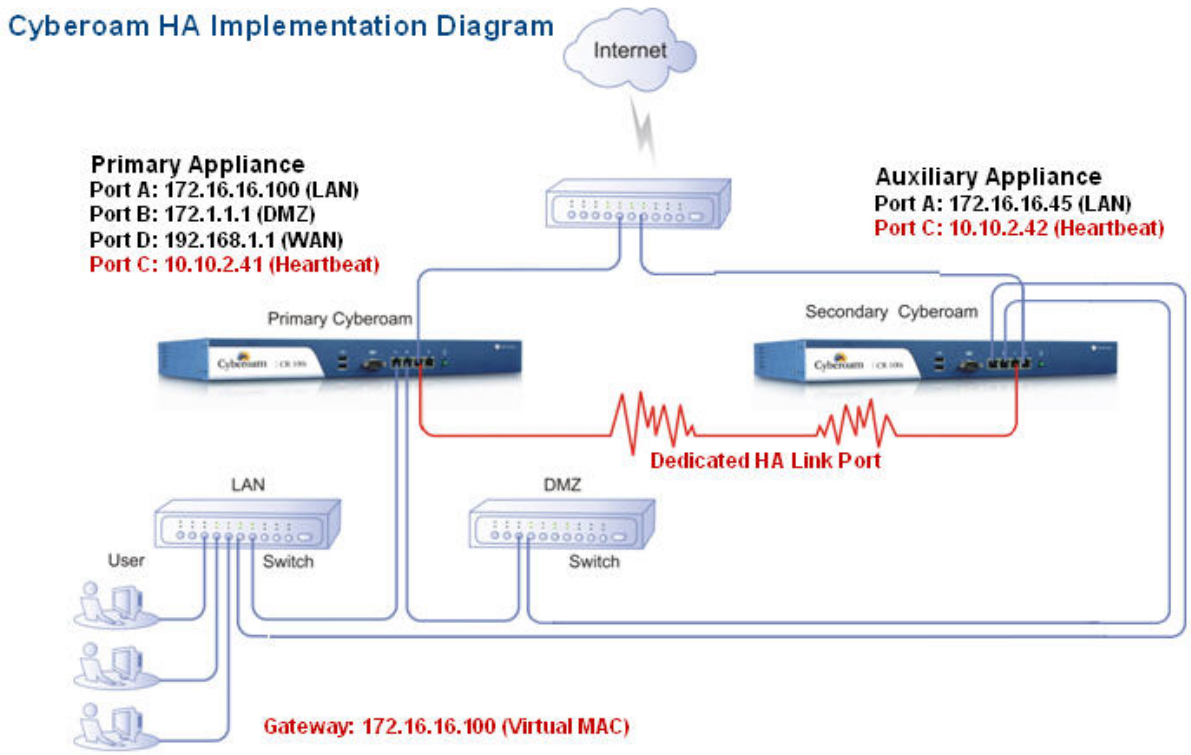
Appliances - primary and auxiliary appliance, are physically connected over a dedicated HA link port.

Typically, traffic enters your network by passing through a network switch. In an HA solution, one of the appliance in the cluster has a Virtual MAC address and traffic is forwarded to the cluster appliance which has the virtual MAC address. The appliance which has virtual MAC address is the Primary Appliance and other peer is Auxiliary Appliance. Primary Appliance acts as a load balancer and forwards the traffic to the Auxiliary Appliance for processing. Auxiliary Appliance can process traffic only if cluster is operating in the Active-Active mode.

If configured in Active-Passive mode, primary appliance processes the entire traffic Auxiliary Appliance waits in a ready mode to operate as the primary appliance, in case primary appliance or any of the monitored links fail.

Auxiliary Appliance monitors the primary appliance through the dedicated HA link and if it does not receive any communication within the pre-configured time, the primary appliance is considered to have failed. In this case, Auxiliary appliance takes ownership of the virtual MAC address from primary appliance, and becomes primary appliance temporarily. Primary appliance automatically takes over from the Auxiliary appliance once it starts functioning.

Below given diagram, displays how two appliances – primary and secondary appliance will be connected physically.



Before configuring HA

Behavior

1. **Features not configurable**

   DHCP, PPPoE, WWAN, WLAN

2. **No Session Failover** for

   AV Scanned sessions or any other forwarded traffic like ICMP, UDP, multicast and broadcast traffic, traffic passing through Proxy Subsystem - transparent, direct and parent proxy traffic, and VPN traffic

3. **Drop Masqueraded Connections**

   In case of Manual Synchronization

4. **Load balanced traffic**

   Normal Forwarded TCP Traffic, NATed (both SNAT & Virtual host) Forwarded TCP Traffic, TCP Traffic Passing through Proxy Subsystem - Transparent Proxy, Direct Proxy, Parent Proxy and VLAN traffic.

5. **Traffic not Load balanced**

   VPN sessions, UDP, ICMP, multicast, and broadcast sessions and scanned FTP traffic. TCP traffic for Web Admin Console or Telnet Console and, H323 traffic sessions

6. **Dedicated HA link port**

   Dedicated HA link port should be from any of the DMZ zone interface only. Make sure that the IP address of HA link port of Primary and Auxiliary appliances are in same subnet.

7. **Deployment Wizard**

   Deployment Wizard of Auxiliary appliance will not be accessible.

8. **Access to Web Admin console of Auxiliary appliance**

   Super Administrator privileges are required to access Auxiliary appliance Web Admin console i.e. it can be accessed by “ADMIN” user only and Live users/DHCP leases/IPSec live connections pages will not be displayed.

9. **Backup & Restore**

- It is not required to disable HA to restore backup.
- After enabling HA if backup without HA configuration is restored then HA will be disabled and primary appliance will be accessible as per the backup configuration while appliance will be accessible with the Auxiliary Admin IP address.

10. **Disable HA**

- HA can be disabled from either of the appliances. If disabled from Primary appliance, HA will be disabled on both the appliances. If disabled from Auxiliary appliances, HA will not be disabled on Primary appliance and will act as stand-alone appliance.
- If HA is disabled from Stand-alone machine, IP schema will not change.
- After disabling HA, Primary appliance IP schema will not change.
- After disabling HA, for Auxiliary appliance, all the ports except dedicated HA link port and Peer Administration port will be disabled. Dedicated HA link port will be assigned Peer HA link IP and Peer Administration port will be assigned Peer Administration IP.
- After disabling HA, for Auxiliary appliance, for LAN zone all the administrative service – HTTP, HTTPS, Telnet, SSH is allowed while for DMZ zone only HTTPS and SSH is allowed.

Limitations

- Not available in models CR15i, CR15wi and CR25i.
- Not supported if appliance is deployed in Bridge mode
- HA will get disabled if you run Deployment Wizard on Primary appliance.
- Quarantine and Spam digest are not consolidated for primary and auxiliary appliance. Hence user will receive digest form both the appliances.

- Appliance cannot be upgraded without disabling HA.

Before configuring HA

Before attempting to configure two Cyberoam appliances as a HA pair for Hardware Failover, check the following requirements:

- Cluster appliances - primary and Auxiliary appliances, must be registered and must be on same version.
- Separate licenses for Cluster appliances. On both the appliances, same subscription modules should be enabled else, these modules will not be supported in the event of a failure of the Primary appliance. For example, if IPS module is enabled at Primary appliance and not enabled on Auxiliary appliance then on failover when Auxiliary appliance becomes Active, IPS policies will not be applicable.
- Cables to all the monitored ports on the both the appliances should be connected. Connect Dedicated HA link port of both the appliances with crossover cable.
- Dedicated HA link port should be from the DMZ zone interface only and should have unique IP address on both the appliances. You can change DMZ IP address from Deployment Wizard.
- Disable DHCP, PPPoE, WWAN and WLAN if configured before HA configuration.

Configure Primary appliance

Prerequisite

Allow SSH traffic for dedicated HA link port on both the appliances through firewall rule or Appliance Access.

1. Select **System → HA → HA**

   Appliance key is the Primary Appliance key while Peer Appliance key is the Auxiliary Appliance key that is displayed only after HA is configured.
2. Select HA Configuration mode for cluster.

   Active-Active Select to configure a cluster for load balancing and failover HA. In active-active mode both primary and auxiliary appliances processes traffic and monitors the status of the other cluster appliance. The primary appliance controls load balancing among both the cluster appliances.

   Active-Passive Select to configure a cluster for failover HA. In active-passive mode the primary appliance processes all connections. Auxiliary appliance passively monitors the cluster status and remains synchronized with the primary appliance.
3. Specify dedicated HA link port. HA peers are physically connected using a crossover cable through this port. You must use the same port as an HA link port on peer appliance also. For example, if you are configuring port E as HA link port on Primary appliance then use port E only as HA link port on Auxiliary appliance. Make sure that the IP address of HA link port of Primary and Auxiliary appliances are in same subnet. Cluster appliances use this link to communicate cluster information and to synchronize with each other.

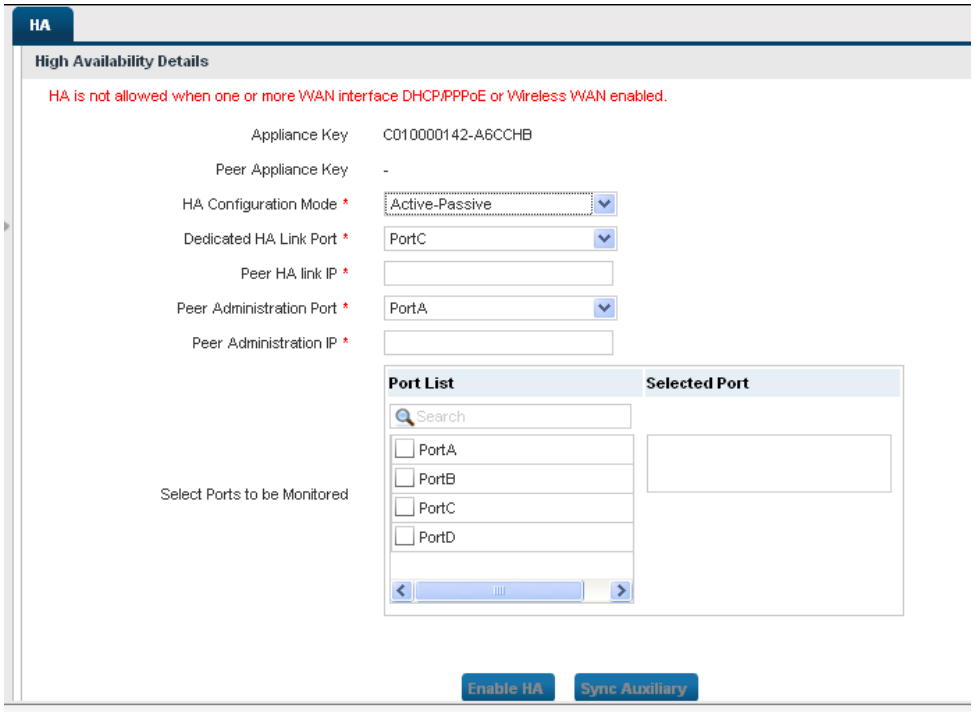
   Dedicated HA link port should be from any of the DMZ zone interface only.
4. Specify IP address configured on the HA link port of the peer appliance.
5. Specify Administration Port of peer appliance i.e. the peer appliance port on which the access is allowed for administration purpose.
6. Specify Administration IP address of the peer appliance. Administrative privileges are required to access Web Admin Console of the Auxiliary appliance i.e. user should login as ADMIN.
7. Select the ports to be monitored. Both the appliances will monitor their own ports and if any of the monitored port goes down, appliance will remove itself from the cluster and failover will occur.
8. Click “Enable HA” button to enable HA

The appliance from which HA is enabled will act as a primary appliance while the peer appliance will act as auxiliary appliance.

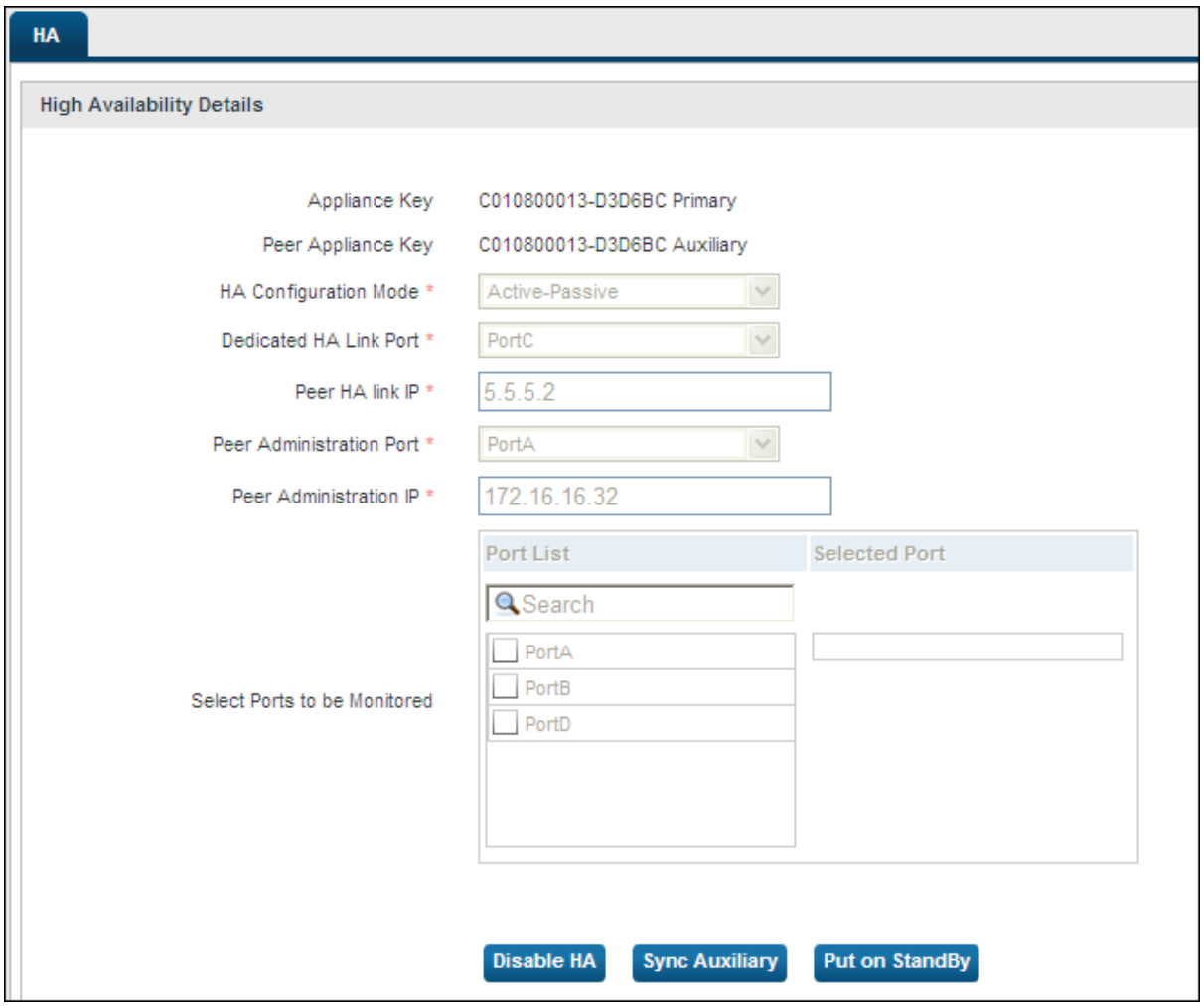
If everything is cabled and configured properly and HA is enabled successfully:

- As per the configuration mode, ‘Active’ will be displayed for Primary appliance and ‘Passive’ or ‘Active’ for Auxiliary appliance
- Both the appliances will have the same configuration except the HA link port IP address.
- Additional options made available after HA is enabled:

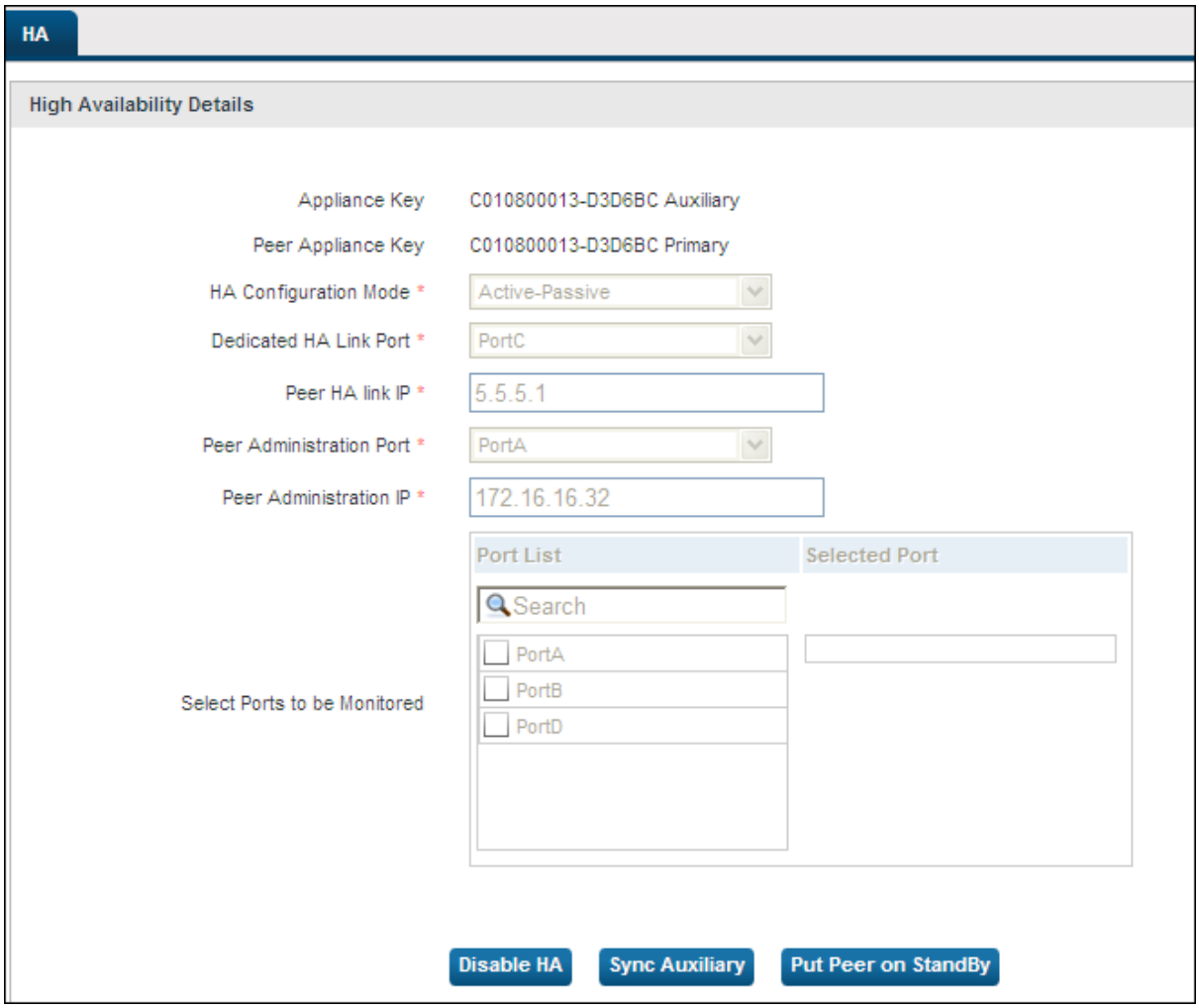
  Primary Appliance – Put on Standby (only for Active-Passive mode), Disable HA, Sync Auxiliary (use to synchronize Auxiliary appliance and Primary appliance configurations)
- By default, as soon as HA is enabled successfully, both the appliances will synchronize automatically.
- As soon as Active-Active is configured, traffic load balancing is enabled. If required, it can be disabled from CLI console using “cyberoam ha load-balancing” command.



Screen – Configure HA



Screen – Primary Appliance (Active – Passive HA)

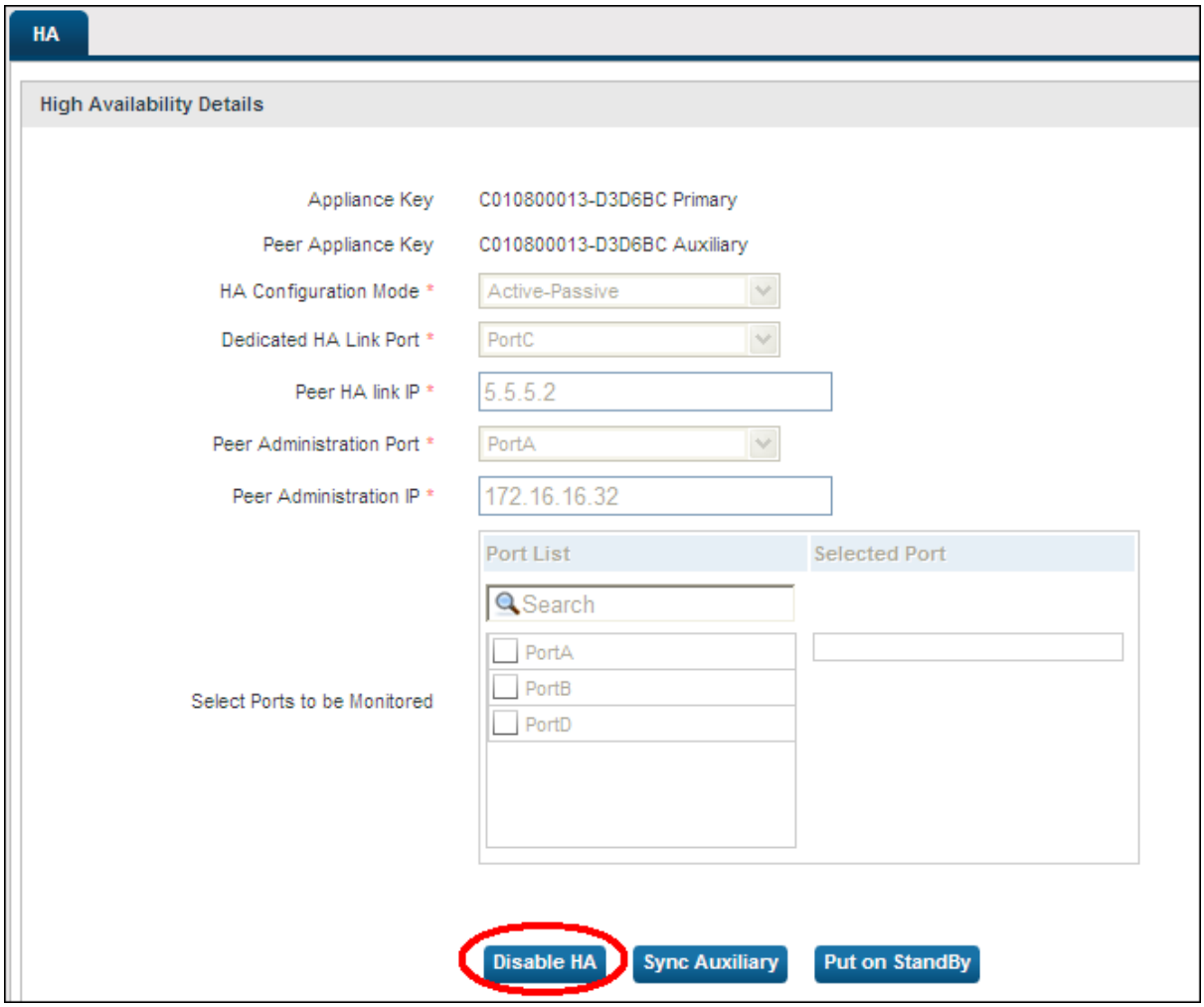


Screen – Auxiliary Appliance (Active – Passive HA)

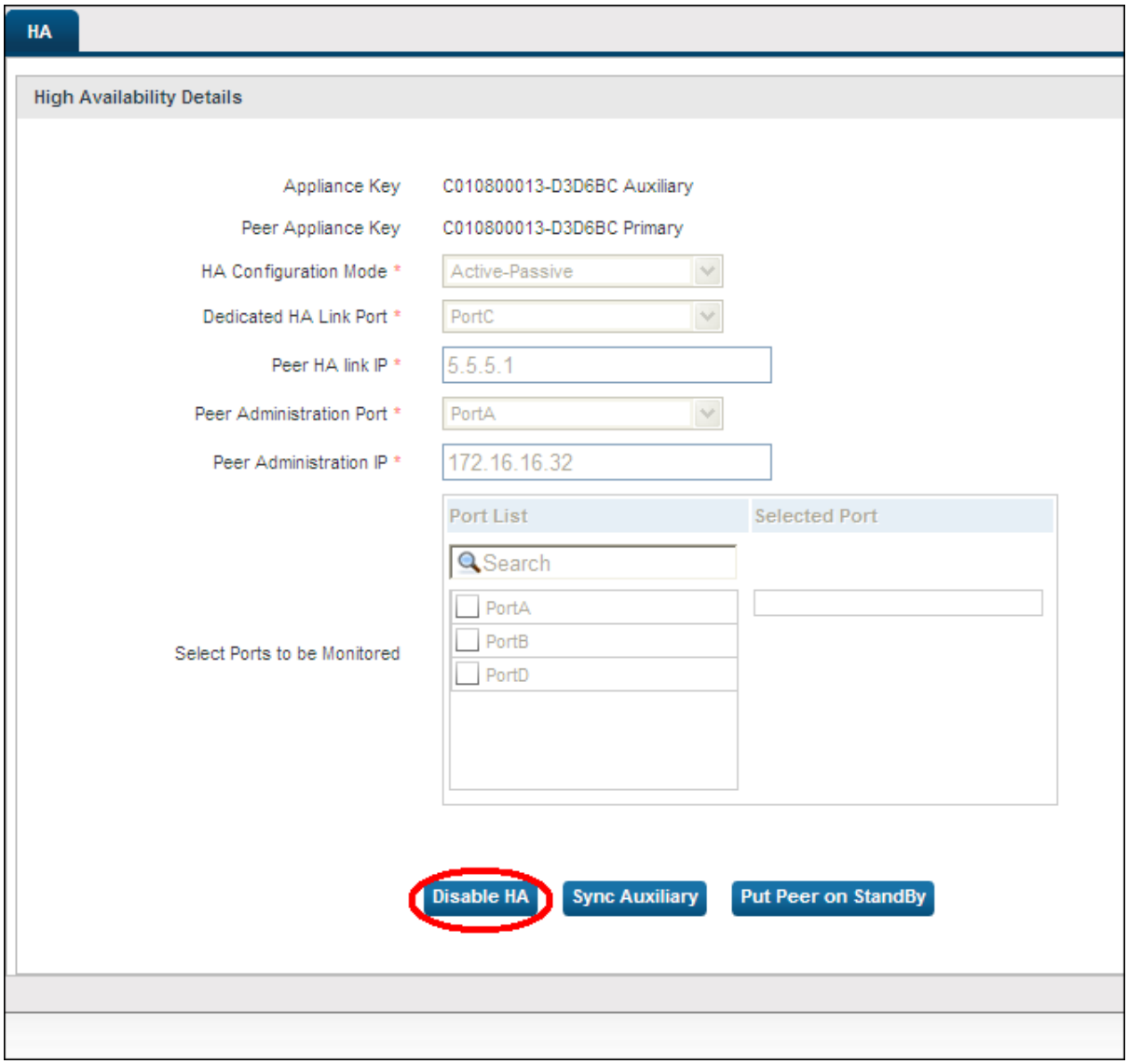
Disable HA

HA can be disabled from HA configuration page (**System → HA → HA**) from primary appliance.

- HA can be disabled from either of the appliances. If disabled from Primary appliance, HA will be disabled on both the appliances. If disabled from Auxiliary appliances, HA will not be disabled on Primary appliance and will act as stand-alone appliance.
- After disabling HA, Primary appliance IP schema will not change.
- After disabling HA, for Auxiliary appliance, all the ports except dedicated HA link port and Peer Administration port will be disabled. Dedicated HA link port will be assigned Peer HA link IP and Peer Administration port will be assigned Peer Administration IP.
- If HA is disabled from Stand-alone machine, IP schema will not change.



Screen – Primary Appliance



Screen – Auxiliary Appliance

Switch Appliance to Standby mode

Standby mode for the appliance can be configured only if cluster is operating in Active-Passive mode. In this mode, auxiliary appliance takes over as primary appliance.

Synchronize Peers

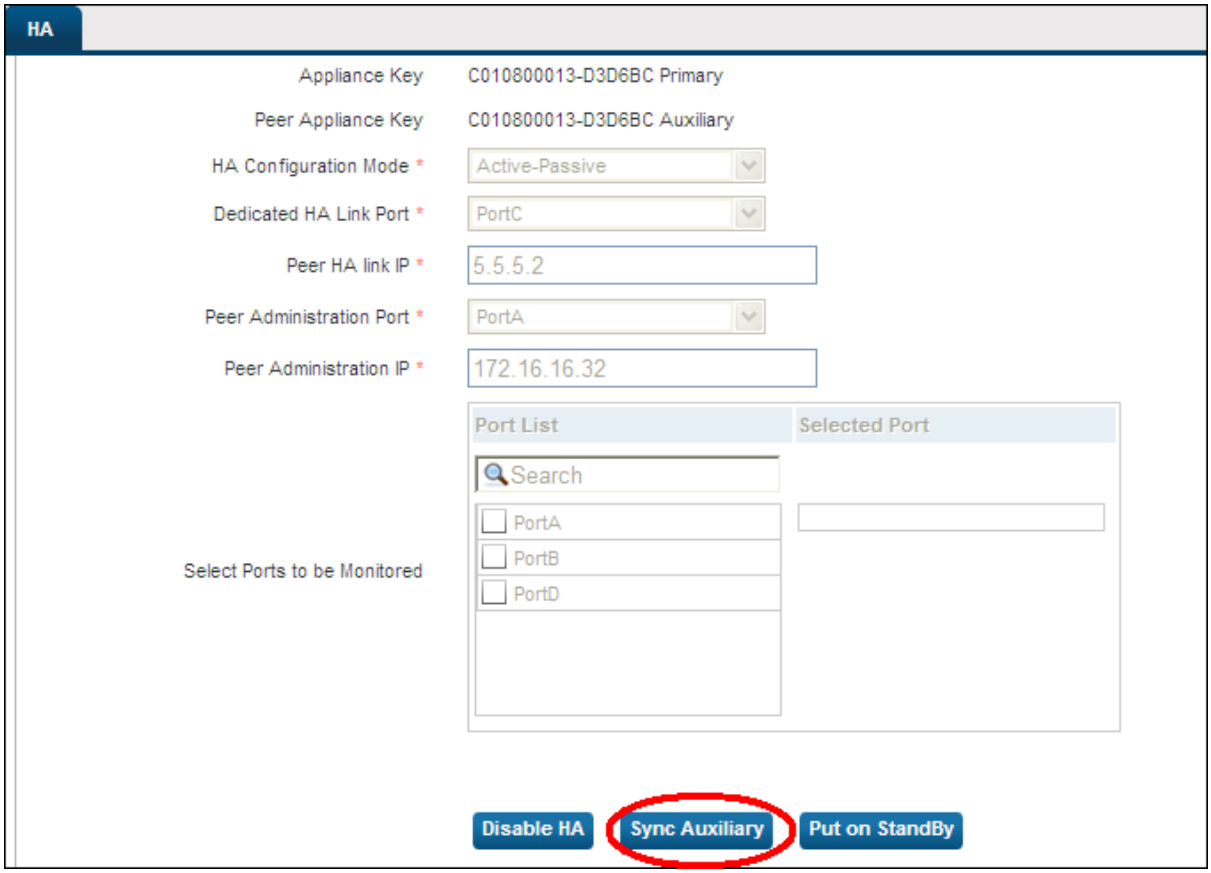
In normal conditions, Auxiliary appliance is always be synchronized with the Primary appliance. But if need arises, Auxiliary appliance can also be forcefully synchronized with the Primary appliance.

Manual synchronization gets the data and configuration updates except reports from the primary appliance.

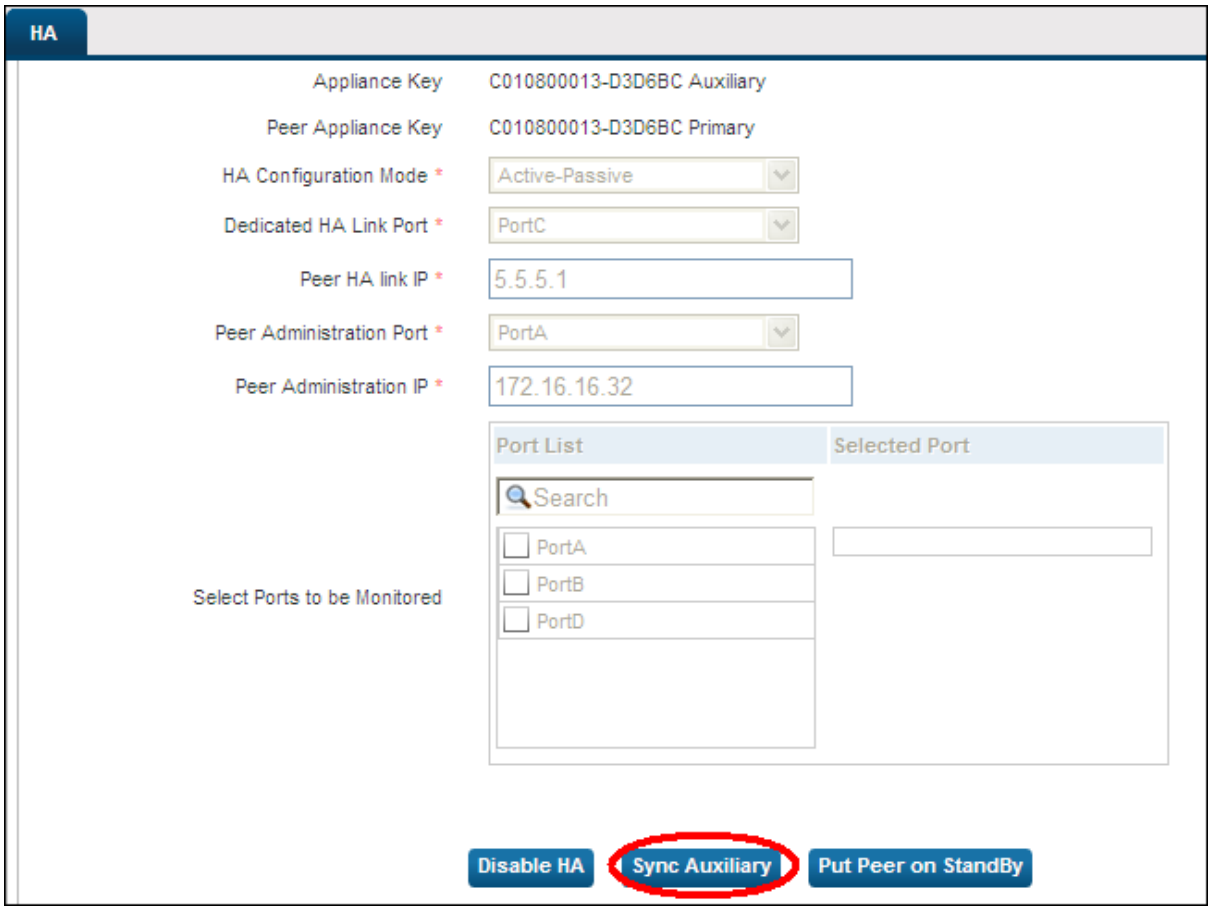
Manual synchronization process can be initiated from either of the cluster appliances from

System → HA → Configure HA page.

If synchronized from primary appliance, primary appliance will push updated and if synchronized from auxiliary appliance, auxiliary appliance will pull the updates from primary appliance.



Screen – Synchronization (from Primary Appliance)



Screen – Synchronization (from Auxiliary Appliance)