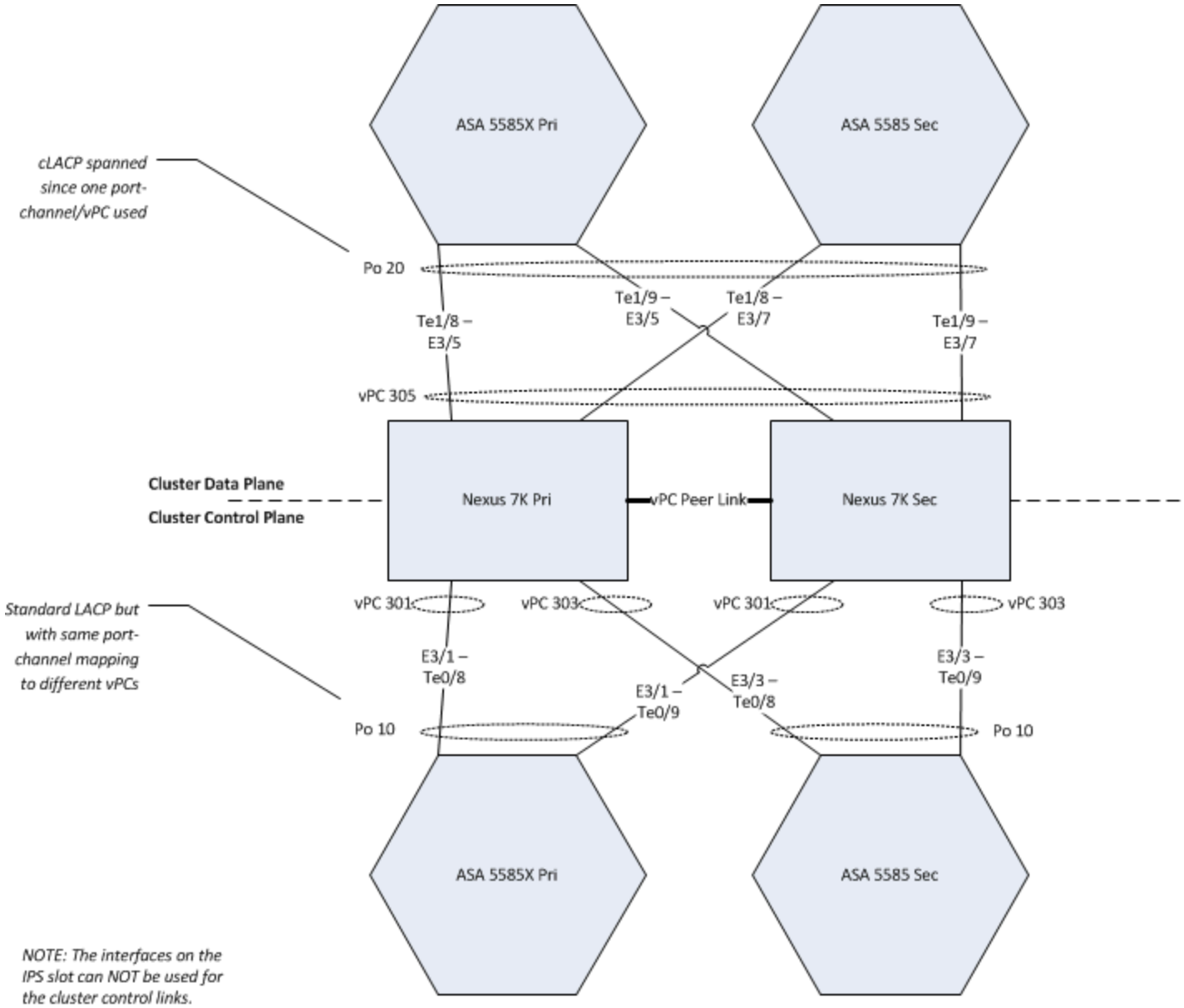
Multi Context Configuration on Clustered Cisco ASA Firewalls

References:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00808d2b63.shtml

The configuration below relates to the design shown in the diagram below:



General Notes

You can not share an interface across contexts. So your management interface can not be allocated to multiple contexts. It's best to just allocate the management interface to the admin

context. Also, you can create sub-interfaces on the management interface but you can NOT assign the same VLAN (i.e. the management VLAN in your organization) to these sub-interfaces, since they need to be on different subnets. So in order to manage individual contexts directly, it is best to just use the first BVI interface in each context as the management address for that context (in addition to data interface).

Multi-Context Configuration

```
! change the mode of the firewall to multiple context mode
! make sure you have the management interface address assigned
! this management address will be used to log into the (admin context
of the) firewall after the mode is changed
! NOTE: IF YOU WILL BE USING TRANSPARENT FIREWALL, YOU MUST CHANGE
FIREWALL TO TRANSPARENT BEFORE CHANGING THE MODE

ciscoasa# config t
ciscoasa(config)# mode multiple
     WARNING: This command will change the behavior of the device
     WARNING: This command will initiate a Reboot
     Proceed with change mode? [confirm]
     Convert the system configuration? [confirm]
     !
     The old running configuration file will be written to flash

     Converting the configuration - this may take several minutes
     for a large configuration

     The admin context configuration will be written to flash

     The new running configuration file was written to flash
     Security context mode: multiple

     ***
     *** --- SHUTDOWN NOW ---
     ***
     *** Message to all terminals:
     ***
     ***   change mode

! after the firewall reboots, log in and you will be placed in the
admin context, which is created by default
ciscoasa/admin#
```

```
! change to system context, where you can see/create contexts and
resource classes and allocate interfaces etc.
ciscoasa/admin# changeto system
ciscoasa#

! create a resource class and limit resources as appropriate
ciscoasa(config)# class silver
ciscoasa(config-class)# limit-resource conns 20%
ciscoasa(config-class)# limit-resource rate conns 1000

! create a context and assign to a specific resource class
ciscoasa(config)# context dmzpub
Creating context 'dmzpub'... Done. (2)
ciscoasa(config-ctx)# member silver

! create empty port channels
ciscoasa(config)# interface port-channel 10
ciscoasa(config-if)# description control path

ciscoasa(config)# interface port-channel 20
ciscoasa(config-if)# description data path

! assign port channel to physical interfaces
ciscoasa(config)# int tenGigabitEthernet 0/8
ciscoasa(config-if)# channel-group 10 mode on
ciscoasa(config-if)# int tenGigabitEthernet 0/9
ciscoasa(config-if)# channel-group 10 mode on

! assign port channel to physical interfaces
ciscoasa(config)# int tenGigabitEthernet 1/8
ciscoasa(config-if)# channel-group 20 mode active
ciscoasa(config-if)# int tenGigabitEthernet 0/9
ciscoasa(config-if)# channel-group 10 mode active

! create sub-interfaces on port channel
ciscoasa(config)# inter port-channel 20.411
ciscoasa(config-subif)# vlan 411
ciscoasa(config)# inter port-channel 20.909
ciscoasa(config-subif)# vlan 909

! assign interfaces to context and specify config file
ciscoasa(config)# context dmzpub
ciscoasa(config-ctx)# allocate-interface port-channel10.411 vlan411
```

```
ciscoasa(config-ctx)# allocate-interface port-channel10.909 vlan909
ciscoasa(config-ctx)# config-url disk0:/dmzpub.cfg
     WARNING: Could not fetch the URL disk0:/dmzpub.cfg
     INFO: Creating context with default config

! change to new context and save config so it will be stored in flash
ciscoasa# changeto context dmzpub
ciscoasa/dmzpub# wr mem
```

===

Layer 2 Configuration
---
http://www.networkingnut.net/configuring-asa-in-transparent-mode/

http://blog.ciscoinferno.net/transparent-and-routed-asa-basics

Cluster Configuration

```
! configure the cluster links on both firewalls
FWL001#
interface TenGigabitEthernet0/8
 description *** to SWT001 E3/1 and E3/3
 channel-group 10 mode on

interface TenGigabitEthernet0/9
 description *** to SWT002 E3/1 and E3/3
 channel-group 10 mode on

interface Port-channel10
 description *** control plane to Nexus 7K

FWL002#
interface TenGigabitEthernet0/8
 description *** to SWT001 E3/1 and E3/3
 channel-group 10 mode on

interface TenGigabitEthernet0/9
 description *** to SWT002 E3/1 and E3/3
 channel-group 10 mode on
```

```
interface Port-channel10
 description *** control plane to Nexus 7K

! configure the nexus side for vPCs
SWT001#
interface port-channel301
  description Etherchannel to FWL001 (Control Plane)
  switchport access vlan 257
  vpc 301
interface Ethernet3/1
  description FWL001-Te0/8 (Control Plane)
  switchport access vlan 257
  udld enable
  channel-group 301 mode on

interface port-channel303
  description Etherchannel to FWL002 (Control Plane)
  switchport access vlan 257
  vpc 303
interface Ethernet3/3
  description FWL002-Te0/8 (Control Plane)
  switchport access vlan 257
  udld enable
  channel-group 303

SWT002#
interface port-channel301
  description Etherchannel to FWL001 (Control Plane)
  switchport access vlan 257
  vpc 301
interface Ethernet3/1
  description FWL001-Te0/9 (Control Plane)
  switchport access vlan 257
  udld enable
  channel-group 301 mode on

interface port-channel303
  description Etherchannel to FWL002 (Control Plane)
  switchport access vlan 257
  vpc 303
interface Ethernet3/3
  description FWL002-Te0/9 (Control Plane)
  switchport access vlan 257
```

```
  udld enable
  channel-group 303

! check the port-channel status on ASA. It will show not in use but
that is OK
FWL001#    sho port-channel summ
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        U - in use      N - not in use, no aggregation/nameif
        M - not in use, no aggregation due to minimum links not met
        w - waiting to be aggregated
Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+---------+------------+-----------------------
-----------
10     Po10(N)            -            No     Te0/8(P)   Te0/9(P)

! configure management interface on the primary firewall
FWL001#
changeto context admin

ip local pool mgmtpool 172.22.100.202-172.22.100.209

interface management0/0
  ip address 172.22.100.201 255.255.255.0 cluster-pool mgmtpool

! configure clustering group on primary firewall
FWL001#
changeto system
! mtu cluster 1600
cluster group ASA
 local-unit FWL001
 cluster-interface port-channel 10 ip 99.99.99.1 255.255.255.240
 priority 1
 key AsaKey
 console-replicate
 enable
! at this stage the port channel should show up state
! enable command above must be done through console session

! configure clustering group on other member(s)
FWL002#
```

```
! remove management ip address
changeto context admin
interface m0/0
 no ipaddress

changeto system
! mtu cluster 1600
cluster group ASA
 local-unit FWL002
 cluster-interface port-channel 10 ip 99.99.99.2 255.255.255.240
 priority 2
 key AsaKey
 console-replicate
 enable as-slave

! I had to issue the enable command twice then you should see some
output showing all extra configuration from slave unit is removed
INFO: This unit will be enabled as a cluster slave without sanity
check and confirmation.
Detected Cluster Master.
Beginning configuration replication from Master.
INFO: ...
WARNING: ...
End configuration replication from Master.
Cluster unit FWL002 transitioned from DISABLED to SLAVE

! cluster should now show both units
FWL001(cfg-cluster)# sho cluster info
Cluster ASA-Cluster: On
     Interface mode: spanned
     This is "FWL002" in state SLAVE
     ID        : 1
     Version   : 9.0(2)
     Serial No.: ...
     CCL IP    : 99.99.99.2
     CCL MAC   : 30e4.db19.6636
     Last join : 09:28:25 UTC May 10 2013
     Last leave: N/A
Other members in the cluster:
     Unit "FWL001" in state MASTER
     ID        : 0
     Version   : 9.0(2)
     Serial No.: ...
```

```
      CCL IP     : 99.99.99.1
      CCL MAC    : 44d3.ca34.fae2
      Last join : 09:05:02 UTC May 10 2013
      Last leave: N/A

! configure data interfaces
! physical interfaces connect to individual nexus switches
```
! NOTE: In order for port-channel trunk links to work, i.e. data links, you MUST disable VLAN tagging on the Nexus switch. This is a global command on Nexus so take caution since it will affect all trunk links. The command to issue on the Nexus switches is 'no vlan dot1q native tag enabled'
```
! See following for above issue:
```
http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/interface_start.html#wp1326437
```
! The ASA does not support LACPDUs that are VLAN-tagged. If you enable
native VLAN tagging on the neighboring switch using the Cisco IOS vlan
dot1Q tag native command, then the ASA will drop the tagged LACPDUs.
Be sure to disable native VLAN tagging on the neighboring switch. In
multiple context mode, these messages are not included in a packet
capture, so you cannot diagnose the issue effectively.

interface TenGigabitEthernet1/8
 description *** to AHQSWT001 E3/5 and E3/7
 channel-group 20 mode active vss-id 1

interface TenGigabitEthernet1/9
 description *** to AHQSWT002 E3/5 and E3/7
 channel-group 20 mode active vss-id 2

! port channel is specified as a 'spanned' port channel
interface Port-channel20
 description *** data plane to Nexus 7K
 port-channel span-cluster vss-load-balance

! NOTE: you will get the following warning
! WARNING: Strongly recommend to configure a virtual MAC address for
span-cluster port-channel interface Po20 or all its subinterfaces in
order to achieve best stability of span-cluster port-channel during
unit join/leave.
INFO: lacp port-priority on member interfaces of channel-group
Port-channel20 will be controlled by CLACP.
INFO: CLACP vss-load-balance is enabled, this assume all cluster
```

```
units have same interfaces connected to two switches in the VSS or
VPC and each unit has same number of interfaces connected to two
switches (vss-id 1 and 2).

! now create sub-interfaces on the port channel
interface Port-channel20.403
 vlan 403
interface Port-channel20.404
 vlan 404
interface Port-channel20.503
 vlan 503
interface Port-channel20.504
 vlan 504

! allocate sub-interfaces to contexts
context dmzpri1
  allocate-interface Port-channel20.403 vlan403
  allocate-interface Port-channel20.404 vlan404
context dmzpub1
  allocate-interface Port-channel20.503 vlan503
  allocate-interface Port-channel20.504 vlan504

! change to context and configure interfaces
changeto context dmzpri1
interface BVI1
 ip address 172.24.2.4 255.255.255.0

interface vlan403
 nameif vlan403
 bridge-group 1
 security-level 100

interface vlan404
 nameif vlan404
 bridge-group 1
 security-level 0

changeto context dmzpub1
interface BVI1
 ip address 172.25.2.4 255.255.255.0
!
interface vlan503
 nameif vlan503
```

```
 bridge-group 1
 security-level 100
!
interface vlan504
 nameif vlan504
 bridge-group 1
 security-level 0
```

Zero-Downtime Upgrade on ASA Cluster
Reference: http://www.cisco.com/en/US/docs/security/asa/asa91/release/notes/asarn91.html

```
! Backup config from each context
write mem all

! Then in each context
write net

! do the following commands in system context
cluster exec copy tftp://<TFTP Server IP Address>/<filename>.bin
disk0:/<filename>.bin

! if a boot system variable value already exists make sure to remove
it so the new value will be at the top
boot system disk0:/<filename>.bin

!verify boot variable values
show boot

! verify current cluster info
Master(config)# sho cluster info
Cluster ASA-Cluster: On
    Interface mode: spanned
    This is "FWL002" in state MASTER
        ID        : 1
        Version   : 9.0(2)
        Serial No.: JAF1516AKEE
        CCL IP    : 99.99.99.2
        CCL MAC   : 30e4.db19.6636
        Last join : 04:21:10 EST Jun 7 2013
        Last leave: 04:19:50 EST Jun 7 2013
Other members in the cluster:
    Unit "FWL001" in state SLAVE
        ID        : 0
```

```
        Version   : 9.0(2)
        Serial No.: JAF1534ABAD
        CCL IP    : 99.99.99.1
        CCL MAC   : 44d3.ca34.fae2
        Last join : 09:17:30 EST Jun 10 2013
        Last leave: 09:12:27 EST Jun 10 2013
FWL001(config)#

FWL001(config)# cluster exec unit FWL001 reload noconfirm
FWL001(config)#

! Cluster will show other unit not present
FWL001(config)# sho cluster info
Cluster ASA-Cluster: On
    Interface mode: spanned
    This is "FWL002" in state MASTER
        ID        : 1
        Version   : 9.0(2)
        Serial No.: JAF1516AKEE
        CCL IP    : 99.99.99.2
        CCL MAC   : 30e4.db19.6636
        Last join : 04:21:10 EST Jun 7 2013
        Last leave: 04:19:50 EST Jun 7 2013
Other members in the cluster:
    There is no other unit in the cluster
FWL001(config)#

! Other unit will come back and join the cluster
FWL001(config)#
Beginning configuration replication to Slave FWL001
 End Configuration Replication to slave.

FWL001(config)# sho cluster info
Cluster ASA-Cluster: On
    Interface mode: spanned
    This is "FWL002" in state MASTER
        ID        : 1
        Version   : 9.0(2)
        Serial No.: JAF1516AKEE
        CCL IP    : 99.99.99.2
        CCL MAC   : 30e4.db19.6636
        Last join : 04:21:10 EST Jun 7 2013
        Last leave: 04:19:50 EST Jun 7 2013
```

```
Other members in the cluster:
    Unit "FWL001" in state SLAVE
        ID        : 0
        Version   : 9.1(2)
        Serial No.: JAF1534ABAD
        CCL IP    : 99.99.99.1
        CCL MAC   : 44d3.ca34.fae2
        Last join : 12:02:14 EST Jun 10 2013
        Last leave: 11:58:34 EST Jun 10 2013
FWL001(config)#

! Now upgrade the master unit

FWL001(config)# reload noconfirm
```