APPLICATION NOTES

Next-Gen Security Architecture through Brocade Network Devices and Palo Alto Networks Firewall

This solution leverages interoperable and best-of-breed networking and security products, tailored to fit individual enterprise requirements.
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Overview</td>
<td>4</td>
</tr>
<tr>
<td>Interoperability Test Results</td>
<td>4</td>
</tr>
<tr>
<td>Reference Architecture</td>
<td>6</td>
</tr>
<tr>
<td>Brocade Router Configuration</td>
<td>8</td>
</tr>
<tr>
<td>Aggregate Layer Brocade NetIron Configuration (Brocade MLX 1)</td>
<td>8</td>
</tr>
<tr>
<td>Access Layer Brocade FastIron Configuration (Brocade FCX 1)</td>
<td>11</td>
</tr>
<tr>
<td>Brocade FastIron Configuration (Brocade FCX 3)</td>
<td>12</td>
</tr>
<tr>
<td>Brocade VDX Configuration (Brocade VDX 1)</td>
<td>13</td>
</tr>
<tr>
<td>Brocade ServerIron ADX Configuration (Brocade Internal ADX) enable</td>
<td>16</td>
</tr>
<tr>
<td>Palo Alto Networks Firewall GUI Configuration</td>
<td>18</td>
</tr>
<tr>
<td>Firewall 2: Configuration</td>
<td>18</td>
</tr>
<tr>
<td>Management</td>
<td>18</td>
</tr>
<tr>
<td>Zones</td>
<td>19</td>
</tr>
<tr>
<td>Virtual Routers</td>
<td>19</td>
</tr>
<tr>
<td>Interfaces</td>
<td>20</td>
</tr>
<tr>
<td>Firewall 2: SNMP and RADIUS</td>
<td>21</td>
</tr>
<tr>
<td>Firewall 2: HIGH AVAILABILITY</td>
<td>21</td>
</tr>
<tr>
<td>Brocade Network Advisor Integration</td>
<td>22</td>
</tr>
<tr>
<td>Appendix A: Brocade ServerIron ADX with Palo Alto Networks Firewall</td>
<td>25</td>
</tr>
<tr>
<td>Pair</td>
<td></td>
</tr>
<tr>
<td>Brocade ServerIron ADX Configuration (External ADX)</td>
<td>25</td>
</tr>
<tr>
<td>Brocade ServerIron ADX Configuration (Internal ADX)</td>
<td>27</td>
</tr>
<tr>
<td>Palo Alto Networks Firewall ADX Configuration (10.17.95.168)</td>
<td>28</td>
</tr>
<tr>
<td>Appendix B: Brocade ServerIron ADX with Palo Alto Networks Layer 2</td>
<td>33</td>
</tr>
<tr>
<td>Firewall Pair in Virtual Wire Mode</td>
<td></td>
</tr>
<tr>
<td>Brocade ServerIron ADX Configuration (External ADX)</td>
<td>33</td>
</tr>
<tr>
<td>Brocade ServerIron ADX Configuration (Internal ADX)</td>
<td>34</td>
</tr>
<tr>
<td>Palo Alto Networks Firewall ADX Configuration (10.17.95.168)</td>
<td>35</td>
</tr>
</tbody>
</table>
INTRODUCTION
Brocade and Palo Alto Networks™ are partnering to deliver a comprehensive solution for High Availability (HA) Secure Networking with the high-density Brocade® NetIron® MLX® Series routers, Brocade VDX® Series Data Center Switches, Brocade ServerIron® ADX Series application load balancers, and Palo Alto Networks firewalls. This joint solution brings end-to-end networking and security to the enterprise networks, campus networks and data centers.

About Palo Alto Networks
Palo Alto Networks is the network security company. Its next-generation firewalls enable unprecedented visibility and granular policy control of applications and content—by user, not just IP address—at up to 20 Gbps with no performance degradation.

For Palo Alto Networks support:
• Phone support in the U.S.: +1.866.898.9087
• International support: http://www.paloaltonetworks.com/literature/datasheets/Support_services_ds.pdf
• E-mail support: support@paloaltonetworks.com
• Web support: https://support.paloaltonetworks.com/

About Brocade
Brocade is a leading provider of high-performance data center, enterprise, and service provider networking solutions and services. Brocade develops extraordinary networking solutions that enable today’s complex, data-intensive businesses to optimize information connectivity and maximize the business value of their data. The Brocade ServerIron ADX Series of application delivery and traffic management switches is the industry leader in high availability, acceleration, security, and scalability for business-critical IP and Web applications.

For Brocade support:
• Phone support in the U.S.: 1-800-752-8061
• International support: www.brocade.com/services-support/contacts_international.page
• E-mail support: ipsupport@brocade.com
• Web support: www.brocade.com/services-support
OVERVIEW
To achieve a secure and highly available network, you can deploy pairs of Brocade NetIron MLX Series routers in a Multi-Chassis Trunking (MCT) configuration with inline firewalls, along with a pair of Brocade ServerIron ADX Series load balancers, to provide highly scalable perimeter security. In an MCT configuration, both routers actively load balance traffic. The MCT operation provides redundancy in the event that a Brocade NetIron MLX router becomes unavailable, while enhancing performance by using both switches to process and forward traffic.

This solution is an example of a secure networking solution. Each pair of Brocade NetIron MLX Series switches provide redundant load balancing, while inline firewalls provide the next generation of capabilities, enabling enterprises to identify and control applications and users and prioritize risk factors. In a perimeter security scenario, the Brocade ServerIron ADX load balances stateful firewall sessions across multiple Palo Alto Networks firewalls. Additionally, Palo Alto Networks firewalls can also be deployed as segmentation gateways in Brocade VCS® enabled data centers to provide zero trust network architecture.

Interoperability Test Results
The interoperability compliance testing that was done covered features, functionality, and serviceability between Brocade switches and Palo Alto Networks firewalls. Different deployment scenarios using Palo Alto Networks firewalls and Brocade ServerIron ADX configurations are briefly discussed in the appendices. The following compliance tests were conducted:

- **Trunking.** A two-link 802.3ad link aggregation was created between the Brocade NetIron MLX and each Palo Alto Networks firewall. The test confirmed that the 802.3ad trunk could be negotiated and form a trunk with each Palo Alto Networks firewall positioned between the Brocade MLX switches. To test failover, one of the trunk links was disconnected, and it was confirmed that traffic continued to flow on the other link.

- **Multi-Chassis Trunking (MCT).** MCT was enabled on Brocade NetIron MLX routers, and it was confirmed that MCT load balanced between the paths. MCT allows links that are physically connected to two Brocade MCT-aware switches to appear to downstream devices as coming from a single device, as part of a single link aggregation group (LAG) trunk interface. Traditional LAG trunks do not provide switch-level redundancy. If the switch to which the LAG trunk is attached fails, the entire LAG trunk loses network connectivity. With MCT, member links of the LAG are connected to two MCT-aware switches, which are directly connected using an Inter-Chassis Link (ICL), to enable data flow and control messages between the switches.

- **Spanning Tree.** Spanning Tree Protocol (STP) was enabled on all Brocade FastIron® switches, and it was confirmed that Spanning Tree converged when the path went down.

- **Virtual Router Redundancy Protocol–Extended (VRRP-e).** VRRP-e was enabled on the Brocade NetIron routers, and redundancy was provided for the Palo Alto Networks firewall to the network.

- **Routing protocols.** Routing protocols (Open Shortest Path First [OSPF], Intermediate System-to-Intermediate System [IS-IS], and Multiprotocol Label Switching [MPLS]) were deployed to verify the interoperability between the Palo Alto Networks firewall and the Brocade routers and switches. To test basic Layer 3 (L3) functionalities, one of the hosts passed traffic via the Internet through Palo Alto Networks firewalls to the test network, and it was confirmed that traffic continued to flow. Traffic was uninterrupted when there was link failure as the network converged.

- **High Availability (HA).** Palo Alto Networks firewalls were tested for HA in active/passive pairs. If the active firewall fails for any reason, the passive firewall becomes active automatically with no loss of service. A failover is triggered when one or more monitored interfaces fail, or when one or more specified destinations cannot be
pinged by the active firewall. Also, if the active device does not respond to heartbeat polls, then the passive device takes over.

- **Application visibility and control.** Application visibility is a tab in the Palo Alto Networks Web control. It provides insight into the exact type of application (Facebook, Gmail, syslog, and so on) that passes through the network. In testing, the Application Command Center (ACC) provided a clear view of applications, bandwidth usage, and the risk factors associated with the current application session. Firewalls were able to warn the administrator or take action according to the policies set when high-threat packets (BitTorrent, FTP, Skype) passed through the network. Policies were deployed to redirect or block high-risk traffic.

- **Brocade Network Advisor.** Brocade Network Advisor is the Brocade network management tool that handles both IP and Storage Area Network (SAN) devices. In testing, the Palo Alto Networks firewalls were discovered by Brocade Network Advisor. Brocade Network Advisor was able to receive traps from the firewall and manage the firewall.

- **Firewall load balancing.** Brocade ServerIron ADXs were deployed between Palo Alto Networks firewalls to test firewall load balancing. This test was conducted under continuous traffic flow.

- **VCS Fabric interop testing.** Tests were conducted with Brocade VDXs and Palo Alto Networks firewalls to test their interoperability.

- **Media types.** Tests were conducted with copper interfaces, along with Ethernet SPFs (Small Form-Factor Pluggables).

- **Port configuration.** Different port speeds were used: Auto-Negotiate and 1000-Full.
REFERENCE ARCHITECTURE

The solution components are listed below and shown in Figure 1 and Figure 2:

- 2 × Brocade NetIron MLX-16s (v5.2c routing code)
- 3 × Brocade FastIron CX Series (v7.3 routing code)
- 2 × Palo Alto Networks Firewall Enterprise (PA-4060, v4.0.9)
- 2 × Brocade ServerIron ADX 1000 (v12.3.1 routing code)
- 4 × Ethernet SFPs (Brocade or Palo Alto Networks)
- 2 × Windows Server 2003 SP2s – (Brocade Network Advisor v11.1.0 and Microsoft AD)

![Diagram of firewall interoperability test architecture with Brocade LAN cloud.](image-url)

**Figure 1.** Firewall interoperability test architecture with Brocade LAN cloud.
Figure 2. Firewall interoperability test architecture with Brocade ServerIron ADX load balancers.
BROCADE ROUTER CONFIGURATION

Aggregate Layer Brocade NetIron Configuration (Brocade MLX 1)

telnet@MLX_1#sh run
Current configuration:
!
ver V5.1.0bT163
module 2 ni-mlx-20-port-1g-copper
!
# Trunk configuration
lag "2" dynamic id 2
    ports ethernet 2/3
    primary-port 2/3
    deploy
!
lag "3" dynamic id 3
    ports ethernet 2/2
    primary-port 2/2
    deploy
!
lag "to MLX_2" dynamic id 1
    ports ethernet 2/4 to 2/5
    primary-port 2/4
    deploy
!
no spanning-tree
!
vlan 1 name DEFAULT-VLAN
    no untagged ethe 2/1
!
vlan 2
    tagged ethe 2/1 to 2/3
!
vlan 20
    tagged ethe 2/9
    router-interface ve 20
!
vlan 30
    tagged ethe 2/9
    router-interface ve 30
!
vlan 200
    tagged ethe 2/1 to 2/3 ethe 2/7
    router-interface ve 22
!
vlan 300
    tagged ethe 2/1 to 2/3 ethe 2/7
    router-interface ve 33
!
vlan 4090 name Session-VLAN
    tagged ethe 2/1
    router-interface ve 100
!
clock summer-time
clock timezone us Pacific
logging console
telnet server
web-management http
web-management https
web-management allow-no-password
ip route 10.0.0.0/8 10.17.80.1
!
# SNMP configuration
snmp-server
snmp-server community ..... ro
snmp-server community ..... rw
snmp-server contact umamageswari
snmp-server host 10.17.95.160 version v1 ..... hostname MLX_1
!
# Layer 3 configuration for routing protocols for IPv4 and IPv6 (OSPF and IS-IS)

router ospf
area 0
!
router isis
net 49.2828.1112.1112.1112.00
is-type level-2
log adjacency
address-family ipv4 unicast
metric-style wide
exit-address-family
address-family ipv6 unicast
exit-address-family
!

# VRRP-e configuration
router vrrp-extended
!
interface loopback 1
ip ospf area 0
ip router isis
ip address 1.1.1.2/32
!
interface management 1
ip address 10.17.95.162/20
enable
!
interface ethernet 2/2
no route-only
!
interface ethernet 2/3
no route-only
!
interface ethernet 2/4
enable
ip ospf area 0
ip router isis
ip address 2.2.2.2/30
ipv6 address 2002::2/64
!
interface ethernet 2/7
enable
no route-only
!
interface ethernet 2/9
enable
!
interface ethernet 2/10
ip ospf area 0
ip router isis
!
interface ethernet 2/11
enable
ip ospf area 0
ip router isis
ip address 5.5.5.3/24
!
interface ethernet 2/12
ip ospf area 0
ip router isis
!
interface ve 20
ip ospf area 0
ip router isis
ip address 20.20.20.2/24
ip vrrp-extended vrid 20
backup priority 200
ip-address 20.20.20.254
activate
!
interface ve 22
ip ospf area 0
ip router isis
ip address 22.22.22.2/24
ip vrrp-extended vrid 22
backup priority 200
ip-address 22.22.22.254
activate
!
interface ve 30
ip ospf area 0
ip router isis
ip address 30.30.30.2/24
ip vrrp-extended vrid 30
backup priority 200
ip-address 30.30.30.254
track-port e 1/11
track-port e 1/12
activate
!
interface ve 33
ip ospf area 0
ip router isis
ip address 33.33.33.2/24
ip vrrp-extended vrid 33
backup priority 200
ip-address 33.33.33.254
track-port e 1/11
track-port e 1/12
activate
!
interface ve 100
ip address 3.3.3.2/24
!
# MPLS configuration
router mpls
policy
  traffic-eng ospf area 0
mpls-interface e2/4
  ldp-enable
  lsp toMLX_2
to 1.1.1.1
  adaptive
  enable
!
# MCT configuration for load balancing the traffic
cluster TOR 1
  rbridge-id 2
  session-vlan 4090
  member-vlan 2
  member-vlan 200
  member-vlan 300
  icl TOR ethernet 2/1
peer 3.3.3.1 rbridge-id 1 icl TOR
deploy
  client FCX_1
    rbridge-id 100
    client-interface ethernet 2/3
deploy
  client FCX_2
    rbridge-id 200
    client-interface ethernet 2/2
deploy

End

Access Layer Brocade FastIron Configuration (Brocade FCX 1)

BR-telnet@FCX_1#sh run
Current configuration
!
ver 07.2.02eT7e1
!
module 1 fgs-48-port-management-module
module 2 fgs-xfp-2-port-10g-module
!
# STP configuration
global-stp
!
  vlan 1 name DEFAULT-VLAN by port
    spanning-tree
  !
  vlan 2 by port
    tagged ethe 0/1/2 to 0/1/3
    spanning-tree
  !
  vlan 20 by port
    tagged ethe 0/1/1 ethe 0/1/10
    untagged ethe 0/1/11 to 0/1/20
    spanning-tree
  !
  vlan 30 by port
    tagged ethe 0/1/1 ethe 0/1/10
    untagged ethe 0/1/21 to 0/1/30
    spanning-tree
  !
  vlan 200 by port
    tagged ethe 0/1/2 to 0/1/3 ethe 0/1/31 to 0/1/35
    spanning-tree
  !
  vlan 300 by port
    tagged ethe 0/1/2 to 0/1/3 ethe 0/1/36 to 0/1/40
    spanning-tree
  !
  enable telnet authentication
  hostname FCX_1
  ip route 10.0.0.0 255.0.0.0 10.17.80.1
!
# SNMP configuration
  snmp-server community ..... ro
  snmp-server community ..... rw
Brocade FastIron Configuration (Brocade FCX 3)

For testing purposes, the Internet was replaced with a Brocade FastIron router, and traffic was passed from a different subnet.

FCX_3(config)#sh run
Current configuration:
! ver 04.3.01bT7e3
! module 1 fgs-48-port-management-module
! vlan 1 name DEFAULT-VLAN by port
! vlan 50 by port
tagged ethe 0/1/4 to 0/1/5
untagged ethe 0/1/1 to 0/1/2 ethe 0/1/11
router-interface ve 50
!
hostname FCX_3
ip route 10.0.0.0 255.0.0.0 10.17.80.1
!

# SNMP configuration
snmp-server community ..... ro
snmp-server community ..... rw
snmp-server contact umamageswari
snmp-server host 10.17.95.160 version v1 ..... 
clock timezone us Pacific

# Web management configuration
web-management https
web-management allow-no-password

# Routing protocol OSPF configuration
router ospf
  area 0
  !
interface loopback 1
  ip address 6.6.6.6 255.255.255.255
  ip ospf area 0
  !
interface ethernet 0/1/4
  ip ospf area 0
  !
interface ethernet 0/1/5
  ip ospf area 0
  !
interface ethernet 0/1/48
  ip address 10.17.95.170 255.255.240.0
  no ip dhcp-client enable
  !
interface ve 50
  ip address 50.50.50.1 255.255.255.0
  ip ospf area 0
  !
end

Brocade VDX Configuration (Brocade VDX 1)
VDX6720# sh run
diag post rbridge-id 1
  enable
  !
dpod 1/0/1
  !
dpod 1/0/2
  reserve
  !
dpod 1/0/3
  reserve
  !
dpod 1/0/4
  !
dpod 1/0/5
  reserve
  !
logging rbridge-id 1
  raslog console INFO
  !
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class Firmware
switch-attributes 1
  chassis-name VDX6720-24
  host-name VDX6720
!
support rbridge-id 1
  ffdc
!
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community brocade
snmp-server community private
snmp-server host 10.17.95.160 ConvergedNetwork
  version 2c
  !
system-monitor fan threshold marginal-threshold 1 down-threshold 2
system-monitor fan alert state removed action raslog
system-monitor power threshold marginal-threshold 1 down-threshold 2
system-monitor power alert state removed action raslog
system-monitor temp threshold marginal-threshold 1 down-threshold 2
system-monitor compact-flash threshold marginal-threshold 1 down-threshold 0
line vty
  exec-timeout 10
!
zoning enabled-configuration cfg-name ""
zoning enabled-configuration default-zone-access alllaccess
zoning enabled-configuration cfg-action cfg-save
aaa authentication login local
role name admin desc Administrator
role name user desc User
service password-encryption
username admin password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role admin desc Administrator
username user password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role user desc User
cee-map default
  precedence 1
  priority-group-table 1 weight 40 pfc on
  priority-group-table 15.0 pfc off
  priority-group-table 15.1 pfc off
  priority-group-table 15.2 pfc off
  priority-group-table 15.3 pfc off
  priority-group-table 15.4 pfc off
  priority-group-table 15.5 pfc off
  priority-group-table 15.6 pfc off
  priority-group-table 15.7 pfc off
  priority-group-table 2 weight 60 pfc off
  priority-table 2 2 1 2 1 2 2 15.0
  remap fabric-priority priority 0
  remap lossless-priority priority 0
!
fcoe
  fabric-map default
vlan 1002
  priority 3
  virtual-fabric 128
  fcmap 0E:FC:00
  advertisement interval 8000
  keep-alive timeout

! map default
  fabric-map default
  cee-map default

! interface Vlan 1
  no shutdown
!
interface Vlan 20
  no shutdown
!
fabric route mcast rbridge-id 1
!
protocol lldp
  advertise dcbx-fcoe-app-tlv
  advertise dcbx-fcoe-logical-link-tlv
  advertise dcbx-tlv
!
vlan dot1q tag native
port-profile default
vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  switchport trunk native-vlan 1
!
# Interface configuration
interface Management 1/0
  no ip address dhcp
  ip address 10.17.95.171/20
  ip gateway-address 10.17.80.1
  ipv6 address ""
  no ipv6 address autoconfig
!
interface TenGigabitEthernet 1/0/1
  fabric isl enable
  fabric trunk enable
  no shutdown
!
interface TenGigabitEthernet 1/0/2
  fabric isl enable
  fabric trunk enable
  switchport
  switchport mode access
  switchport access vlan 20
  no shutdown
!
interface TenGigabitEthernet 1/0/3
  fabric isl enable
  fabric trunk enable
  switchport
  switchport mode access
  switchport access vlan 20
  no shutdown
!
**Brocade ServerIron ADX Configuration (Brocade Internal ADX)**

```bash
enable
configure terminal
hostname Internal_ADX
!
# The following commands are to configure a virtual interface on VLAN 1. The virtual interface is associated with all the ports in the VLAN. In this case, since all the Brocade ServerIron ADX ports are in the default VLAN, the virtual routing interface is associated with all the ports in the device.
vlan 1
  router-interface ve 1
  exit
  interface ve 1
  ip address 110.10.2.222 255.255.255.0
  exit
  ip route 110.0.0.0 255.0.0.0 110.10.2.5
!
# The following commands add the firewall definitions. In this configuration, port HTTP is configured on each firewall. Specifying the application ports on the firewalls is optional. If you configure an application port in a firewall, load balancing is performed for the configuration port. All the traffic from a given client for ports that are not configured is sent to the same firewall.
server fw-name fw1 110.10.2.5
  port http
  exit
server fw-name fw2 110.10.2.6
  port http
  exit
!
# The following commands add the firewall definitions to the firewall port group (always group 2). The firewall group contains all the ports in VLAN 1 (the default VLAN).
server fw-group 2
  fw-name fw1
  fw-name fw2

# The following commands add the path through the firewalls to the other Brocade ServerIron ADX. Each path consists of a path number, an ADX port number, the IP address at the other end of the path, and the next-hop IP address. In this example, the topology does not contain routers other than the Brocade ServerIron ADXs. If your topology does contain other routers, configure firewall paths for the routers also. For router paths, use the same IP address as the path destination and the next hop. The path IDs must be in contiguous, ascending numerical order, starting with 1.

  fwall-info 1 1 110.10.1.111 110.10.2.5
  fwall-info 2 2 110.10.1.111 110.10.2.6

# The following commands set the load balancing method to balance requests based on the firewall that has the least number of connections for the requested service. Since the firewall definitions above specify the HTTP service, the Brocade ServerIron ADX will load balance requests based on the firewall that has fewer HTTP session entries in the Brocade ServerIron ADX session table.

  fw-predictor per-service-least-conn
  exit

# The following commands add static MAC entries for the firewall interfaces with the Brocade ServerIron ADX. The static MAC entries are required only if the configuration uses static routes and a single virtual routing interface, as in this example, and if the default gateway for the client or server is the firewall. If the configuration uses a dynamic routing protocol (for example, Routing Information Protocol [RIP] or OSPF), the static entries are not required. Alternatively, the static entries are not required if you use the Brocade ServerIron ADX itself as the default gateway for the client or the server. For example, the static entries are not required if you configure the client to use 10.10.1.111 as its default gateway.

  vlan 1
  static-mac-address 001b.1703.6e15 ethernet 1
```
priority 1 router-type
    static-mac-address 001b.1718.8115 ethernet 2
priority 1 router-type
    exit
    write memory

Brocade ServerIron ADX Configuration (Brocade External ADX)

   enable
   configure terminal
   hostname Internal_ADX
   vlan 1
   router-interface ve 1
   exit
   interface ve 1
   ip address 110.10.1.111 255.255.255.0
   exit
   ip route 110.0.0.0 255.0.0.0 110.10.1.5
   server fw-name fw1 110.10.1.5
   port http
   exit
   server fw-name fw2 110.10.1.6
   port http
   exit
   server fw-group 2
   fw-name fw1
   fw-name fw2
   fw-all-info 1 1 110.10.2.222 110.10.1.5
   fw-all-info 2 2 110.10.2.222 110.10.1.6
   fw-predictor per-service-least-conn
   exit
   vlan 1
   static-mac-address 001b.1703.6e14 ethernet 1
   priority 1 router-type
   static-mac-address 001b.1718.8114 ethernet 2
   priority 1 router-type
   exit
   write memory
After configuring the Brocade NetIron and FastIron routers and switches, you need to log in to the firewall and configure it using the Palo Alto Networks Firewall Enterprise Admin Console. The following sections describe how to configure internal and external interfaces, routing, rules, Simple Network Management Protocol (SNMP) traps, and High Availability (HA) on the two firewalls via the management interface.

**Firewall 2: Configuration**

You can use any web browser to login into Firewall GUI. The Dashboard is the first screen that appears when you log in to the Firewall Web Console. The Dashboard gives a summary of the devices, which includes general information about the device, HA and interface status, and logs and resource information.

![Palo Alto Networks Firewall: Dashboard](image)

**Management**

You must do a basic configuration of the Palo Alto Networks firewall to provide access to the Web console. Configure the management interfaces of any Palo Alto Networks firewall by directly using an Ethernet cable to management interface and then establishing an SSH (Secure Shell) session to the device with an IP address of 192.168.1.1/24. Once the IP address is set, log in through a Web browser, using the default username/password `admin/admin`. A Palo Alto Networks firewall requires configuration of virtual routers and zones before configuring interfaces for Layer 3 (L3) deployment.

**Zones**

A typical perimeter firewall deployment has three zones, a “Trust,” a “DMZ (Demilitarized),” and an "Untrust” zone. To allow traffic to pass through the firewall from the internal network to the Internet, a policy that permits traffic between the “Trust” and “Untrust” zones is required. Zones are particularly useful for internal segmentation, when you need to control traffic and protect resources between different groups or functions.

Configure the zones of the Palo Alto Networks Firewall 2:

Palo Alto Networks Firewall2 > Network > Zones > New
For this configuration, the following zone configurations are added:
Name of zone: L3-trust
Type: Layer 3
Interfaces: ethernet 1/5 and loopback

Click OK, and then click Commit to save and run the change.

Virtual Routers
These are required for a Layer 3 deployment. This is where static routes are added and where dynamic routing protocols are configured. All Layer 3 interfaces must be created and a default route added. Each virtual router maintains a separate set of routes.

Configure the virtual routers of Palo Alto Networks Firewall 2:
Palo Alto Networks Firewall2 > Network > Virtual Routers> New
For this configuration, the following virtual router configurations are added:

Virtual Router: Default
OSPF tab
Router ID: 5.5.5.1
Add new area using 0.0.0.0 (which is area 0).
Add OSPF Network in the Export Rules – 50.50.50.0/24 via ext-2 link.

Click **OK**, and then click **Commit** to save and run the change.

**Interfaces**

Palo Alto Networks firewalls support both physical and logical interfaces, and all interfaces must be configured to belong to a zone before traffic can pass between two interfaces. Multiple interfaces can belong to a single zone, but a logical interface can belong only to a single zone. Palo Alto Networks devices support virtual LAN (VLAN) tagging (802.1Q), so a single physical interface can have several logical subinterfaces, each in its own custom zone.

Configure the interfaces of Palo Alto Networks Firewall 2:
Palo Alto Networks Firewall2 > Network > Interfaces > ethernet 1/5

![Figure 6. Palo Alto Networks Firewall: Interface configuration](image)

For this configuration, the following interface configurations are added:

Ethernet Name: ethernet 1/5
IP Address: 5.5.5.1/24
Virtual Router: Default
Zone: L3-trust

Click **OK**, and then click **Commit** to save and run the change.
Firewall 2: SNMP and RADIUS

You can add one or more SNMP, RADIUS, LDAP, syslog, and e-mail servers.

Configure the SNMP server for Palo Alto Networks Firewall 2:
Palo Alto Networks Firewall2 > Devices > SNMP > New

Figure 7. Palo Alto Networks firewall: SNMP server configuration

For this configuration, the following SNMP server configurations are added:

Server Name: SNMP Server
Name: BNA (for Brocade Network Advisor)
Manager IP: 10.17.95.160
Community: brocade

Click RADIUS on the left panel under Server Profile, and click New to add a RADIUS server.

Click OK, and then click Commit to save and run the change.

Firewall 2: HIGH AVAILABILITY

You can deploy firewalls in active/passive pairs, so that if the active firewall fails for any reason, the passive firewall becomes active automatically with no loss of service. A failover can also occur if selected Ethernet links fail or if the active firewall cannot reach one or more of the specified destinations. To set up HA, follow these steps:

Step 1. Use two firewalls with the same model number.

Step 2. Connect the passive firewall to your network and the Internet using the same physical ports as the active firewall.

Step 3. Using two crossover RJ-45 Ethernet cables, connect the HA1 and HA2 ports on the passive firewall to the HA1 and HA2 ports on the active firewall, or connect the ports on both firewalls to a switch.

Step 4. Configure the relevant data, in this case, the IP address: 10.0.0.1 255.255.255.252, the Peer IP: 10.0.0.2 255.255.255.252, and the Passive Link State: shutdown.

Step 5. Configure a similar configuration on the passive firewall.
Figure 8. Palo Alto Networks firewall: HA configuration

NOTES:

• In an active/passive pair, both firewalls must be the same model and must have the same licenses. If state synchronization is enabled, sessions continue after a switchover; however, threat prevention functions do not continue.

• On the Palo Alto Networks PA-2000 Series and PA-500 firewalls, you specify the data ports to use for HA. On the PA-4000 Series, there are dedicated physical ports for HA.

• On the PA-2000 and PA-500 Series, you must use the traffic interfaces for HA. For example, connect the ethernet1/15 interfaces to each other and the ethernet1/6 interfaces to each other.

• For a detailed description on HA, please refer to the document, “How to Configure HA on PAN-OS.”

Brocade Network Advisor Integration

Brocade Network Advisor can manage Palo Alto Networks devices by compiling Palo Alto Networks firewall-specific Management Information Bases (MIBs). Following is a brief description of the steps in the Brocade Network Advisor integration process:

1. Load the Palo Alto Networks MIBs in a new folder (PAN) under
   \C:\Program Files > Network Advisor 11.1.0 > conf > mibs > ip > PAN

2. Add the MIBs along with their path to the mibs_to_compile.txt file in
   \C:\Program Files > Network Advisor 11.1.0 > conf > mibs
3. Register any unregistered traps in Monitor > SNMP Setup > Event Reception

4. Discover the device Discover > IP Products > Add (under the Discovered tab). Enter the IP address and community string to add the device.
5. Discovered devices are seen under the IP tab.

Figure 12. Brocade Network Advisor: Trap reception

Figure 13. Brocade Network Advisor: Discovery of Palo Alto Networks firewall, Brocade VDX™, Brocade FCX.
Figure 14. Test architecture of Brocade ServerIron ADX and Palo Alto Networks Firewall in HA pair (active/passive).

Brocade ServerIron ADX Configuration (External ADX)

!Building configuration...
!Current configuration : 1804 bytes
!
ver       12.3.01dT403
!
global-protocol-vlan
!
context default
!
!
server fw-name fw1 110.10.1.5
  port http
  port http url "HEAD /"
!
server fw-name fw2 110.10.1.6
  port http
  port http url "HEAD /"
server fw-group 2
12-fwwall

sym-priority 250
fw-name fw1
fw-name fw2

fwall-info 1 1 110.10.2.5 110.10.1.5
default-router
fwall-info 2 2 110.10.2.5 110.10.1.5
fwall-info 3 3 110.10.2.6 110.10.1.6
default-router
fwall-info 4 4 110.10.2.6 110.10.1.6

fw-predictor per-service-least-conn

vlan 1 name DEFAULT-VLAN by port
always-active
router-interface ve 1
!
eventlog size 256
no enable aaa console
hostname EXT_ADX
ip route 10.0.0.0 255.0.0.0 10.17.80.1
default-router
default-router
ip route 110.0.0.0 255.0.0.0 110.10.1.5
default-router
ip route 110.0.0.0 255.0.0.0 110.10.1.6
!
logging 10.17.95.160
telnet server
username admin password ..... 
snmp-server community ..... ro
snmp-server community ..... rw
snmp-server host 10.17.95.160 ..... 
!
interface management 1
ip address 10.17.95.164 255.255.255.240.0
!
interface ve 1
ip address 110.10.1.111 255.255.255.255
!
end
Brocade ServerIron ADX Configuration (Internal ADX)

!Building configuration...
!Current configuration : 1118 bytes
!
ver      12.3.01dT403
!
global-protocol-vlan
!
context default
!
!
server fw-name fw1 110.10.2.5
   port http
   port http url "HEAD /"
!
server fw-name fw2 110.10.2.6
   port http
   port http url "HEAD /"
!
server fw-group 2
   l2-fwall

   sym-priority 250
   fw-name fw1
   fw-name fw2

   fwall-info 1 1 110.10.1.5 110.10.2.5
   fwall-info 2 2 110.10.1.5 110.10.2.5
   fwall-info 3 3 110.10.1.6 110.10.2.6
   fwall-info 4 4 110.10.1.6 110.10.2.6

   fw-predictor per-service-least-conn
   vlan 1 name DEFAULT-VLAN by port
   always-active
   router-interface ve 1
!
eventlog size 256
aaa authentication web-server default local
no enable aaa console
hostname INT_ADX
ip route 10.0.0.0 255.0.0.0 10.17.80.1
ip route 110.0.0.0 255.0.0.0 110.10.2.5
ip route 110.0.0.0 255.0.0.0 110.10.2.6
!
logging 10.17.95.160
telnet server
username admin password ..... 
snmp-server community ..... ro
snmp-server community ..... rw
snmp-server host 10.17.95.160 ..... 
!
interface management 1
   ip address 10.17.95.163 255.255.240.0
!
interface ve 1
   ip address 110.10.2.222 255.255.255.0

End
Palo Alto Networks Firewall ADX Configuration (10.17.95.168)

admin@PA-4060(active)# show network

    network {
        interface {
            ethernet {
                ethernet1/1 {
                    virtual-wire;
                }
                ethernet1/2 {
                    virtual-wire;
                }
                ethernet1/5 {
                    link-speed auto;
                    link-duplex auto;
                    link-state auto;
                    layer3 {
                        mtu 1500;
                        interface-management-profile "Allow All";
                        ip {
                            110.10.1.6/24;
                        }
                        ipv6 {
                            enabled no;
                            neighbor-discovery {
                                enable-dad no;
                            }
                        }
                    }
                }
                ethernet1/6 {
                    link-speed auto;
                    link-duplex auto;
                    link-state auto;
                    layer3 {
                        mtu 1500;
                        interface-management-profile "Allow All";
                        ip {
                            110.10.2.6/24;
                        }
                        ipv6 {
                            enabled no;
                            neighbor-discovery {
                                enable-dad no;
                            }
                        }
                    }
                }
                ethernet1/7 {
                    link-speed auto;
                    link-duplex auto;
                    link-state auto;
                    layer3 {
                        mtu 1500;
                        interface-management-profile "Allow All";
                        ip {
                            20.20.20.5/24;
                        }
                    }
                }
            }
        }
    }
ethernet1/3 {
  link-speed auto;
  link-duplex auto;
  link-state auto;
  layer3 {
    mtu 1500;
    interface-management-profile "Allow All";
    ip {
      40.40.40.1/24;
    }
  }
}

loopback {
  units;
  mtu 1500;
  ip [15.0.0.1];
  interface-management-profile "Allow All";
}
vlan {
  units;
}
tunnel {
  units;
}

vlan {
  20 {
    virtual-interface {
      interface vlan;
      l3-forwarding yes;
    }
  }
}

virtual-wire {
  default-vwire {
    interface1 ethernet1/1;
    interface2 ethernet1/2;
    tag-allowed 0;
    multicast-firewalling {
      enable no;
    }
    link-state-pass-through {
      enable yes;
    }
  }
}

profiles {
  monitor-profile {
    default {
      action wait-recover;
      interval 3;
      threshold 5;
    }
  }
  interface-management-profile {

"Allow All" {
  ping yes;
  telnet no;
  ssh yes;
  http no;
  https yes;
  snmp yes;
}
}
qos {
  profile {
    default {
      class1 {
        priority real-time;
      }
      class2 {
        priority high;
      }
      class3 {
        priority high;
      }
      class4 {
        priority medium;
      }
      class5 {
        priority medium;
      }
      class6 {
        priority low;
      }
      class7 {
        priority low;
      }
      class8 {
        priority low;
      }
    }
  }
}
virtual-router {
  default {
    interface [ ethernet1/3 ethernet1/7 loopback ethernet1/5 ethernet1/6];
    routing-table {
      ip;
      ipv6;
    }
    protocol {
      rip {
        enable no;
        reject-default-route no;
        allow-redist-default-route no;
        timers;
      }
      ospf {
        router-id 5.5.5.1;
        enable no;
      }
    }
  }
}
reject-default-route no;
allow-redist-default-route no;
rfc1583 no;
export-rules {
  50.50.50.0/24 {
    new-path-type ext-2;
  }
  40.40.40.0/24 {
    new-path-type ext-1;
  }
}
bgp {
  enable no;
  reject-default-route no;
  routing-options {
    as-format 2-byte;
    med {
      deterministic-med-comparison no;
    }
    graceful-restart {
      enable no;
    }
    aggregate {
      aggregate-med no;
    }
  }
  dampening-profile {
    default {
      enable yes;
      cutoff 1.25;
      reuse 0.5;
      max-hold-time 900;
      decay-half-life-reachable 300;
      decay-half-life-unreachable 900;
    }
  }
  policy {
    aggregation;
  }
}
ike {
  crypto-profiles {
    ike-profiles {
      default {
        encryption [ aes128 3des];
        hash sha1;
        dh-group group2;
        lifetime {
          hours 8;
        }
      }
    }
  }
  ipsec-profiles {
    default {
      esp {


cipher encryption [ aes128 3des];
  authentication sha1;
}
dh-group group2;
lifetime {
  hours 1;
}
}
gateway;
}
tunnel {
  ipsec;
  ssl-vpn;
  global-protect-gateway;
}
}
[edit]
admin@PA-4060(active)#
APPENDIX B: BROCADE SERVERIRON ADX WITH PALO ALTO NETWORKS LAYER 2 FIREWALL PAIR IN VIRTUAL WIRE MODE

Figure 15. Test architecture of Brocade ServerIron ADX and Palo Alto Networks layer 2 Firewall in Virtual Wire mode

Brocade ServerIron ADX Configuration (External ADX)

telnet@External_ADX>sh run
! Building configuration...
! Current configuration : 1500 bytes

ver 12.3.01dT403

! global-protocol-vlan

! context default

!

server fw-name fw1 110.10.2.7
  port http
  port http url "HEAD /"

server fw-name fw2 110.10.2.8
  port http
  port http url "HEAD /"

server fw-group 2
fw-name fw1
fw-name fw2

fwall-info 1 1 110.10.2.222 110.10.2.7
fwall-info 2 2 110.10.2.222 110.10.2.8

fw-predictor per-service-least-conn

vlan 1 name DEFAULT-VLAN by port
route-port router-interface ve 1

! eventlog size 256
aaa authentication web-server default local
no enable aaa console
hostname External_ADX
ip route 110.0.0.0 255.0.0.0 110.10.2.5

! telnet server
username admin password ..... !
interface ve 1
ip address 110.10.2.111 255.255.255.255
ip address 110.10.2.255 255.255.255.255 secondary
ip address 110.10.2.5 255.255.255.255 secondary

--- BEGIN SSH2 PUBLIC KEY ---
Comment: RomCliSecure DSA Public key
AAAAB3NzaC1kc3MAAACBAKZf6qtRHGHjPFOP3drw01m28l4fpN5X5c8ArkeKhV3a
Tyz4O4uwCsSyvYQw/s24E+989MWxLUO0lb+nV+hWIK0nx85bQPILv0jaWNtbgg
OfNdz4VYncLxszsiQgHqGQ3LW2zQ7fsP9pM5AALaS7MDOaSdNj5a68aUgEMY1ta5
AAAAAFQC1r9L5Mkax780F0nwkB6elaNjCWAAAHS97vSxdyRel4IucL4Ckn7y/ZvWFe
LpwHiVP41MN7d02aApuWvsylL/FUAouv/3PRug/bAAS56w2/JLKvvo1aRPNHA
vgPFEDooqLc+dnC1bXFu1VR69ntQYTE6iRelwzeEPLwTW5ucGHddXvbP2jG3R+
JEmGgt87P3xicCjAAAAGHjfsKMIspqWzw8LgyEWl0XcqI/YkchdFSY1aw4U0k
8GdmvHYsRLzcslOLxVMqViy8FXpsKGHg6m49uMimkCWGxUudQG65y21Qs+P
qRNNiGZxchhZ53h7D+SJjdKXknKoF0Vcd2jjlykhXbe4FhVww+zrdN+E5jrjUIWL8
--- END SSH2 PUBLIC KEY ---

! end

Brocade ServerIron ADX Configuration (Internal ADX)

Internal_ADX#sh run
!Building configuration...
!Current configuration : 814 bytes
!
ver 12.3.01dT403
!
global-protocol-vlan
!
context default
!
!
solver fw-name fw1 110.10.2.5
port http
port http url "HEAD /"
Next-Gen Security Architecture through Brocade NetIron Routers and Palo Alto Networks Firewall Application Note

Palo Alto Networks Firewall ADX Configuration (10.17.95.168)

```plaintext
network {
    interface {
        ethernet {
            ethernet1/1 {
                virtual-wire;
            }
            ethernet1/2 {
                virtual-wire;
            }
            ethernet1/5 {
                link-speed auto;
                link-duplex auto;
                link-state auto;
                virtual-wire;
            }
            ethernet1/6 {
                link-speed auto;
                link-duplex auto;
                link-state auto;
                virtual-wire;
            }
        }
    }
}
```

! server fw-name fw2 110.10.2.6
  port http
  port http url "HEAD /*"
! server fw-group 2

fw-name fw1
fw-name fw2

fwall-info 1 1 110.10.2.111 110.10.2.5
fwall-info 2 2 110.10.2.111 110.10.2.6

fw-predictor per-service-least-conn

vlan 1 name DEFAULT-VLAN by port
router-interface ve 1
!
eventlog size 256
aaa authentication web-server default local
no enable aaa console
hostname Internal_ADX
ip route 110.0.0.0 255.0.0.0 110.10.2.5
!
telnet server
username admin password .....  
!
interface ve 1
ip address 110.10.2.222 255.255.255.0
ip address 110.10.2.7 255.255.255.0 secondary
ip address 110.10.2.8 255.255.255.0 secondary
!
end

Palo Alto Networks Firewall ADX Configuration (10.17.95.168)
ethernet1/7 {
  link-state auto;
  layer3 {
    mtu 1500;
    interface-management-profile "Allow All";
    ip {
      20.20.20.5/24;
    }
  }
}

ethernet1/3 {
  link-state auto;
  layer3 {
    mtu 1500;
    interface-management-profile "Allow All";
    ip {
      40.40.40.1/24;
    }
  }
}

loopback {
  units;
  mtu 1500;
  ip {
    15.0.0.1;
  }
  interface-management-profile "Allow All";
}

vlan {
  units;
}

tunnel {
  units;
}

vlan {
  20 {
    virtual-interface {
      interface vlan;
      l3-forwarding yes;
    }
  }
}

tunnel {
  20 {
    virtual-wire {
      interface ethernet1/1;
      interface ethernet1/2;
      tag-allowed 0;
      multicast-firewalling {
        enable no;
      }
      link-state-pass-through {
        enable yes;
      }
    }
    virtual-wire {
      interface ethernet1/5;
    }
  }
}

Next-Gen Security Architecture through Brocade NetIron Routers and Palo Alto Networks Firewall Application Note
interface2 ethernet1/6;
tag-allowed 0;
multicast-firewalling {
  enable no;
}
link-state-pass-through {
  enable yes;
}
}
}
profiles {
  monitor-profile {
    default {
      action wait-recover;
      interval 3;
      threshold 5;
    }
  }
  interface-management-profile {
    "Allow All" {
      ping yes;
      telnet no;
      ssh yes;
      http no;
      https yes;
      snmp yes;
    }
  }
}
}
qos {
  profile {
    default {
      class {
        class1 {
          priority real-time;
        }
        class2 {
          priority high;
        }
        class3 {
          priority high;
        }
        class4 {
          priority medium;
        }
        class5 {
          priority medium;
        }
        class6 {
          priority low;
        }
        class7 {
          priority low;
        }
        class8 {
          priority low;
        }
      }
    }
  }
}
virtual-router {
    default {
        interface [ ethernet1/3 ethernet1/7 loopback];
        routing-table {
            ip;
            ipv6;
        }
    }
}

protocol {
    rip {
        enable no;
        reject-default-route no;
        allow-redist-default-route no;
        timers;
    }
    ospf {
        router-id 5.5.5.1;
        enable no;
        reject-default-route no;
        allow-redist-default-route no;
        rfc1583 no;
        export-rules {
            50.50.50.0/24 {
                new-path-type ext-2;
            }
            40.40.40.0/24 {
                new-path-type ext-1;
            }
        }
    }
    bgp {
        enable no;
        reject-default-route no;
        routing-options {
            as-format 2-byte;
            med {
                deterministic-med-comparison no;
            }
            graceful-restart {
                enable no;
            }
            aggregate {
                aggregate-med no;
            }
        }
        dampening-profile {
            default {
                enable yes;
                cutoff 1.25;
                reuse 0.5;
                max-hold-time 900;
                decay-half-life-reachable 300;
                decay-half-life-unreachable 900;
            }
        }
    }
}
ike {
  crypto-profiles {
    ike-crypto-profiles {
      default {
        encryption [ aes128 3des];
        hash sha1;
        dh-group group2;
        lifetime {
          hours 8;
        }
      }
    }
    ipsec-crypto-profiles {
      default {
        esp {
          encryption [ aes128 3des];
          authentication sha1;
        }
        dh-group group2;
        lifetime {
          hours 1;
        }
      }
    }
  }
}

[edit]
admin@PA-4060#