YOUR CHALLENGE
When choosing a security platform, organizations usually choose between two distinct choices: simplicity or flexibility. If they go with the simplicity of a security appliance, they lose the flexibility to add technologies as their needs change. Or they deploy their security solution on an inexpensive, flexible open server that must be modified, or “hardened,” to make it secure, a process that can be less than simple. With limited financial and IT personnel resources, organizations frequently feel they must choose between simplicity and flexibility.

OUR SOLUTION
The robust Check Point GAiA pre-hardened operating system combines simplicity and built-in security with the flexibility of running the same pre-hardened operating system on open servers or virtualized gateways.

The feature-rich GAiA web and command line interface (CLI) management interfaces are ideal for both novice and advanced users. Inclusion of Industry Standard management interfaces like RADIUS and TACACs+ for authentication and SNMP for monitoring ensures the security device fits seamlessly into the most dynamic management environments. Support of IPv4 and IPv6, dynamic routing protocols and 802.3ad link aggregation ensures the device fits seamlessly into the most complex networks.

With Check Point’s market-leading security solutions and the flexible Software Blade architecture running on the GAiA pre-hardened operating system, resource-constrained IT administrators can quickly deploy comprehensive enterprise-class security with the GAiA platform anywhere in the network.

KEY FEATURES
- Full compatibility with IPSO & SecurePlatform
- Feature-rich user interface
- Native IPv6 security with high connection capacity

KEY BENEFITS
- Combines the best features of IPSO & SPLAT
- Increased operational efficiency
- A secure platform for the most demanding environments
**SECURE PLATFORM FOR APPLIANCES, OPEN SERVERS AND VIRTUALIZED GATEWAYS**

GAiA combines the best technologies of the SecurePlatform and IPSO operating systems to deliver a unified and integrated operating system for all Check Point appliances, open servers and virtualized environments.

<table>
<thead>
<tr>
<th>SecurePlatform</th>
<th>IPSO</th>
<th>VMWare and Open Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="SecurePlatform" /></td>
<td><img src="image2" alt="IPSO" /></td>
<td><img src="image3" alt="VMWare and Open Servers" /></td>
</tr>
</tbody>
</table>

**BENEFITS OF GAiA FOR SECUREPLATFORM AND IPSO USERS**

<table>
<thead>
<tr>
<th>Existing IPSO Users</th>
<th>Existing SecurePlatform Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ease of Use</td>
<td>• Powerful Management</td>
</tr>
<tr>
<td>- Configuration wizards</td>
<td>- WebUI and CLI</td>
</tr>
<tr>
<td>- One-step install</td>
<td>- Role-based administration</td>
</tr>
<tr>
<td>- One-click registration</td>
<td>- Multiple configuration sets</td>
</tr>
<tr>
<td>• Full Software Blade support</td>
<td>• Manageable dynamic routing</td>
</tr>
<tr>
<td>• Higher connection capacity</td>
<td>• Higher connection capacity</td>
</tr>
<tr>
<td>- 64 Bit OS</td>
<td>- 64 Bit OS</td>
</tr>
<tr>
<td>• IPv6 security</td>
<td>• IPv6 security</td>
</tr>
<tr>
<td>- Supports Dual stack and Tunneling</td>
<td>- Supports Dual stack and Tunneling</td>
</tr>
<tr>
<td>- SecureXL and CoreXL acceleration</td>
<td>- SecureXL and CoreXL acceleration</td>
</tr>
<tr>
<td>• More clustering options</td>
<td>• More clustering options</td>
</tr>
<tr>
<td>- ClusterXL or VRRP</td>
<td>- ClusterXL or VRRP</td>
</tr>
<tr>
<td>• Enhanced device management</td>
<td>• Enhanced device management</td>
</tr>
<tr>
<td>- Image snapshot</td>
<td>- Image snapshot</td>
</tr>
<tr>
<td>- Device replication</td>
<td>- Device replication</td>
</tr>
<tr>
<td>• Automated software update</td>
<td>• Automated software update</td>
</tr>
</tbody>
</table>
Full Software Blade Support
Comprehensive security and multi-layered protection is enabled by GAiA and the full suite of Check Point Software Blades it supports. Pre-packaged solutions provide turn-key security for various business deployment scenarios. Software Blades can also be individually selected to build customized solutions to meet specific security needs. Supported Security Gateway Blades include Firewall, IPsec VPN, IPS, Application Control, Mobile Access, DLP, URL Filtering, Antivirus, Anti-spam & Email Security, Anti-Bot, Identity Awareness and Advanced Networking & Clustering. In addition GAiA supports Check Point’s award-winning Security Management Software Blades that integrate policy configuration, monitoring, logging, reporting and security event management in a single interface—helping minimize total cost of ownership.

Example Security Gateway Blades

Full Compatibility with IPSO and SPLAT CLI
Transitioning to GAiA is a breeze for security administrators. The same powerful command line interface (CLI) commands from IPSO and SPLAT are seamlessly integrated into GAiA. Additional new commands and capabilities are also added to the GAiA CLI making a powerful CLI interface even more intuitive to use. For example:

---setting default gateway
set static-route default nexthop gateway address 192.168.29.2 priority 1 on

---adding static routes
set static-route 172.23.124.150/32 nexthop gateway address 192.168.29.50 on

---Add proxy arp
add arp static ipv4-address 192.168.29.56 macaddress 0:a0:8e:7d:13:d0
add arp static ipv4-address 192.168.29.57 macaddress 0:a0:8e:7d:13:d0

---Add an interface
set interface eth1 link-speed 1000M/full state on
set interface eth1c0 ipv4-address 192.168.29.54 mask-length 24
set interface eth1c0 ipv6-address 2607:f0b0:1:3800::1 mask-length 64
set interface eth1c0 state on

---VRRP
set vrrp interface eth1 on
set vrrp coldstart-delay 60

INCREASE OPERATIONAL EFFICIENCY WITH WIDE RANGE OF FEATURES
Web-Based User Interface with Search Navigation
The intuitive WebUI delivers a refreshing user experience for security administrators. This interface integrates all management functions into a Web-based dashboard that is accessible via the most popular Web browsers—Internet Explorer, Chrome, Firefox and Safari. The built-in search navigation delivers instant results on commands and properties. For the CLI-inclined users, a Shell-Emulator pop-up window is only a single click away.

Role-Based Administrative Access
Segregation of duty is part of a good security policy and it improves operating efficiency and auditing of administrative events. The role-based administrative access gives GAiA customers the ability and granular control to customize their security management policies particular to their business needs. Specific levels of access can be granted based on each individual’s role and responsibility—building a stronger security environment.
GAiA commands are organized into features and commands that may be assigned as needed to administrative roles. A feature is a group of related commands. Extended commands provide access to abilities outside the domain of the command line, such as operating system or security gateway utilities. Additional extended commands can be defined by typing "add command".

Support for Industry Standard Authentication Servers
The AAA component of GAiA manages user access to the appliance. Generally, AAA includes Authentication (identifying a user), Authorization (determining what a user is permitted to do), and Accounting (tracking some aspects of a user’s activity). GAiA implements Pluggable Authentication Modules (PAM), an industry-standard framework for authenticating and authorizing users. Using PAM, authentication, account management, and session management algorithms are contained in shared modules.

RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System) are client/server authentication standards that support remote-access applications. GAiA integrates with these centralized databases residing on authentication servers within an enterprise to authenticate GAiA administrators and operators. This includes linking groups for role based access.

Support for Industry Standard Monitoring
GAiA supports the user-based security model (USM) component of SNMPv3 to supply message-level security. With USM described in RFC 3414, access to the SNMP service is controlled on the basis of user identities. Each user has a name, an authentication pass phrase to identify the user, and an optional privacy pass phrase for protection against disclosure of SNMP message payloads. Managed devices use trap messages to report hardware and product events to a Network Management Station (NMS).

Automatic Software Updates
Software updates is an important process to maintain robust security performance and high network integrity. It is also a process that can sometimes cause disruptions to the network services or to your business. With the intelligent software updates offered by GAiA, new releases and patches can be pre-scheduled for automatic download and deployment at a time with minimum business impact. Update times have been reduced to only a few seconds and post-update checks automatically rollback to the previous configuration if a problem is found. Notification emails are sent about new and recommended updates and update statuses.

Automate Security Gateway Deployments
GAiA simplifies the deployment process with a couple of new tools. Create a First-Time Installation Wizard answer file template and then use this to during the deployment process to automatically configure the gateway.

---Create a template for gateway deployment
config_system –create-template <path>

To facilitate IPSO migrations, upgrade one IPSO gateway and create a customized IPSO to GAiA upgrade package. This upgrade package can be used to quickly upgrade multiple gateways without having to repeat the configuration details in the original upgrade. This upgrade package can also be used as a SmartUpdate upgrade package.

SECURE PLATFORM FOR THE MOST DEMANDING ENVIRONMENTS
Native IPv4 and IPv6 Support
With the support of both IPv4 and IPv6 networking protocols GAiA is designed to provide effective and comprehensive security for all modern networks, including the next-generation of IP networks. Support for IPv6 is included with the Acceleration and Clustering Blade. Customers and customers migrating to IPv6 will benefit from the Dual Stack and Tunneling transition methods in GAiA.

Dual Stack is the concept of running IPv4 and IPv6 at the same time in parallel. That is, IPv4 and IPv6 packets will flow over the same wire and are transmitted and received on the same interface. It is still the best transition strategy for most enterprise networks. Security policies can be implemented for IPv6 that match the security policies implemented for IPv4. Internal services can be made available on IPv6 in a gradual manner. Clients that are not able to run IPv6 will still be able to access services via IPv4.
**Tunneling** is the concept of running one protocol over another, for example carrying an IPv6 packet as the data portion of an IPv4 packet. A common use case is a home or small remote office that wants access to IPv6, but the ISP does not yet provide support for IPv6. With GAiA, IPv6 packets can be tunneled inside of IPv4 packets in order to reach the part of the Internet that supports IPv6. An enterprise use case of IPv6 over IPv4 tunnels is to use it to bridge the parts of the Enterprise network that are IPv4 only. GAiA supports configured tunnels “IPv6 in IPv4” (RFC4213) which is the main approach to tunnel IPv6 in IPv4. Similarly, “Generic Packet Tunneling in IPv6” is the main approach to tunnel IPv4 in IPv6. These may be host to host, host to router, or router to router. These tunnels are very similar to VPNs except they do not secure or authenticate the traffic. IPSEC VPN technology can also be used to create secure and/or authenticated tunnels. Unencrypted tunnels are appropriate inside an Enterprise, but using VPN technology is preferred for creating tunnels between the main Enterprise network and remote sites.

**ClusterXL or VRRP Clusters**
Whether your preferred network redundancy protocol is Check Point ClusterXL technology or standard VRRP protocol (RFC 3768), it is no longer a “platform choice” you will have to make with GAiA. Both ClusterXL and VRRP are fully supported by GAiA, and GAiA is available on all Check Point Appliances, open servers and virtualized environments. There are no more trade-off decisions between required network protocols and preferred security platforms/functions. The cluster serves as a single system image router supporting security applications and both static routes and dynamic routing protocols including OSPF, BGP, and PIM-SM/DM. Integral routing helps to create a complete high-availability gateway, manageable as a single-system image.

**High Connection Capacity**
Utilizing the efficiency of a 64-bit operating system, GAiA is capable of boosting connection capacity of existing Check Point Appliances. Boosting connection capacity to 10M concurrent connections on 2012 Appliances, and to 70M concurrent connections on the 61000 Security System, makes it an ideal solution for all network environments—including the high-demanding and high-performance networks. All supported appliances with a minimum of 6 GB of memory will benefit from the increased connection capacity of the 64-bit operating system.

<table>
<thead>
<tr>
<th>Appliance Model</th>
<th>Default/Maximum Memory (GB)</th>
<th>Default/Maximum Concurrent Connections (M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4800</td>
<td>4/8</td>
<td>1.2/3.3</td>
</tr>
<tr>
<td>12200</td>
<td>4/12</td>
<td>1.2/5</td>
</tr>
<tr>
<td>12400</td>
<td>4/12</td>
<td>1.2/5</td>
</tr>
<tr>
<td>12600</td>
<td>6/12</td>
<td>2.5/5</td>
</tr>
<tr>
<td>21400</td>
<td>12/24</td>
<td>5/10</td>
</tr>
<tr>
<td>Power-1 11000</td>
<td>6/6</td>
<td>2.5</td>
</tr>
<tr>
<td>IP 1280</td>
<td>4/8</td>
<td>1.2/3.3</td>
</tr>
<tr>
<td>IP 2450</td>
<td>4/8</td>
<td>1.2/3.3</td>
</tr>
<tr>
<td>Open Servers</td>
<td>Varies/24</td>
<td>Varies/10</td>
</tr>
</tbody>
</table>
Manageable Dynamic Routing Suite
Eleven dynamic routing and multicasting protocols are supported by GAiA providing flexible and uninterrupted network connectivity. All can be managed according to your preference from the Web UI or from the CLI.

<table>
<thead>
<tr>
<th>Dynamic Routing Protocols</th>
<th>Multicast Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP RFC 1058</td>
<td>IGMPv2 RFC 2236</td>
</tr>
<tr>
<td>RIPv 2 (with authentication) RFC 1723</td>
<td>IGMPv3 RFC 3376</td>
</tr>
<tr>
<td>OSPFv2 RFC 2328</td>
<td>PIM-SM RFC 4601</td>
</tr>
<tr>
<td>OSPF NSSA RFC 3101</td>
<td>PIM-SSM RFC 4601</td>
</tr>
<tr>
<td></td>
<td>PIM-DM state refresh draft-ietf-pim-refresh-02.txt</td>
</tr>
</tbody>
</table>

Policy Based Routing
As a network administrator you may want to exert detailed control over traffic forwarding by using policy based routing (PBR). When you use PBR, you create routing tables of static routes and direct traffic to the appropriate tables by using an access control list (ACL). Using an ACL in this way lets you direct traffic flow by filtering on one or more of the following.

- Source address
- Source mask length
- Destination address
- Destination mask length
- Interface

A future version of GAiA will support port or service based PBR.

Link Aggregation
Link Aggregation is a technology that joins multiple physical interfaces into one virtual interface known as a bond interface. The bond interface gives fault tolerance and increases throughput by sharing the load among many interfaces. You can define bond interfaces using one of these functional strategies:

- High Availability (Active/Backup): Gives redundancy when there is an interface or link failure. This strategy also supports switch redundancy in one of these modes:
  - Round Robin—Selects the active slave interface sequentially.
  - Active/Backup—If the active slave interface goes down, the connection automatically fails over to the primary slave interface. If the primary slave interface is not available, the connection fails over to a different slave.

- Load Sharing (Active/Active): Slave interfaces are active simultaneously. Traffic is distributed among the slave interfaces to maximize throughput. Load Sharing does not support switch redundancy. You can configure load sharing using one of these modes:
  - Round Robin—Selects the active slave interface sequentially.
  - 802.3ad—Dynamically uses active slaves to share the traffic load using the LACP protocol. This protocol enables full interface monitoring between the gateway and a switch.
  - XOR—Selects the algorithm for slave selection according to the TCP/IP layer.

NEXT STEPS—MIGRATING TO GAIA
Check Point GAiA is available for evaluation now. Visit the Check Point User Center and the R75.40 Support Page to begin your evaluation today. If you are new to Check Point, visit the Try Our Products page to get a 30 day trial license for evaluating Check Point GAiA.

First Time Installation
Multiple software install options are available including via a DVD or a USB stick. Install the image and run a First Time Installation Wizard from the Web UI or Command Line Interface.

Overview of Upgrading From SecurePlatform
1. Upgrade the product licenses to R75 or higher
2. Connect a DVD drive to the USB port on the computer
3. Run: # patch add cd
4. Select the applicable upgrade option
5. After the upgrade, remove the DVD from the drive
6. Reboot
7. Install a policy

Overview of Upgrading from IPSO
1. Mount the GAiA ISO on an FTP server
2. Install the GAiA upgrade package on the IP Appliance
3. Run the upgrade package
4. Supply backup location (optional)
5. Supply upgrade template (optional)
6. Confirm
7. Script runs automatically