Datasheet:
SmartWorkflow Software Blade

THE CHALLENGE
Today's evolving business needs drive a constant stream of change requests to IT administrators. Businesses require rapid responses to changing needs, from common activities like adding, removing, or modifying employee, partner, and customer access rights to more complex requests such as adding and removing remote offices, or adding and removing network segments. Responding to these requests can put organizations at risk. Implementation of these frequent policy changes across dozens of gateways and devices can lead to configuration errors, increased security risks, network bottlenecks, network downtime, and non-compliance with corporate and industry standards.

These needs cannot be ignored; security managers must be able to implement frequent policy changes without fear of creating an adverse impact to security, network performance, and compliance within their organization.

OUR SOLUTION
The Check Point SmartWorkflow Software Blade provides a seamless and automated process for policy change management that helps administrators reduce errors and enhance compliance. The SmartWorkflow Software Blade provides managers with visual change tracking, flexible authorization, and comprehensive audit and reporting from a single console. The SmartWorkflow Software blade minimizes configuration errors and optimizes the integrity of network security by providing one-stop, total policy lifecycle management.

The SmartWorkflow Software Blade is fully integrated into the Check Point Software Blade Architecture, providing complete visibility and control of changes being implemented across the enterprise. Organizations reduce the risk of unauthorized and unplanned changes by enforcing a formal process for editing, reviewing, approving, and auditing policy changes. This process reduces security policy configuration errors by enabling IT administrators to review which policies will be impacted by proposed changes and comparing planned changes to the current security posture, before the changes are implemented. The SmartWorkflow Software Blade provides audit trails that track the evolution of security policies, and audit ready reports on the change life cycle to further protect the organization from unplanned changes and enhance compliance with corporate and regulatory standards.

PRODUCT FEATURES
- Unified security management console
- Automated security change management
- Visual change tracking and reporting
- Session approval
- Flexible authorization
- Policy revision and summary reports
- Track changes made to objects, security policies, and session events with SmartView Tracker audit logs

PRODUCT BENEFITS
- Increase security
- Reduce downtime
- Automatic, formal process for tracking, approving, and auditing policy changes
- Flexible authorization conforming to established company approval processes
- Maximizes operational efficiency
- Enhances compliance by maintaining visibility and control of constantly evolving policies
- Advanced auditing and reporting tracks the evolution of policy changes
- Streamlined change management reduces errors and saves administrator time
Datasheet: SmartWorkflow Software Blade

CHECK POINT SMARTWORKFLOW SOFTWARE BLADE FEATURES

Single-console for Total Security Change Management
Via the SmartDashboard graphical user interface, the SmartWorkflow Software Blade provides an intuitive and easy-to-use security management console to centrally manage the editing, reviewing, approving and auditing of policy changes.

Automated Security Change Management
Administrators have a constant need to make firewall changes. These changes are often done manually and hurriedly and can result in mis-configurations and duplication of rules. The SmartWorkflow Software Blade helps administrators track these changes in entities called sessions—logical units that contain a set of changes made within SmartDashboard. Administrators can track changes made to rule bases, network objects, security policies, users, administrators, groups, OPSEC applications, VPN communities and servers.

Visual Change Tracking and Reporting
Changes made to rules and objects are easily viewed in SmartDashboard, enabling administrators to review the impact on the entire rule base.

Administrators can scroll through the changes in chronological order or they can generate a summary change report that provides a comprehensive picture of the changes that were made during the current session. Clicking on a link in the “name” column of the summary change report will generate a detailed list of how the specific object has changed, who changed it as well as the previous time it was modified and by whom.

Session Approval & Flexible Authorization
SmartWorkflow adds an extra layer of security by requiring a manager’s approval before installing a changed security policy (the “four-eyes” principle). Authorized managers can either approve the session or request that modifications be made to the session.

In addition, SmartWorkflow can adapt to existing change management approval processes. It can be configured so that only managers can approve a change or the administrator can approve his own changes or, in the case of an emergency, it can be configured so that a policy can be installed without official approval and the appropriate password.

Policy Revisions and Baseline Comparisons
Prior to approving a session, a manager can review the security configuration change summary report and see the objects that were added, changed or deleted and compare these changes to the security policy that is currently installed. In addition, via the SmartDashboard “read-only” mode, managers can review the changes between any two sessions or they can view the changes of a single session.

Audit Trails
SmartWorkflow enables administrators to track changes that have been made to objects, security policies and session events over an extended period of time. These changes are recorded in Check Point SmartView Tracker as audit logs.

Integrated into Check Point Software Blade Architecture
The SmartWorkflow Software Blade is integrated into the Software Blade Architecture. It can be easily and rapidly activated on existing Check Point security management servers, saving time and reducing costs by leveraging existing security infrastructure.
## SOFTWARE BLADE SPECIFICATIONS

<table>
<thead>
<tr>
<th>Feature</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-based Policy Changes</td>
<td>• Security policy changes are done in the context of a session  &lt;br&gt; • Notes can be added to sessions for clarification  &lt;br&gt; • Changes made within a session can be discarded  &lt;br&gt; • Sessions submitted for approval are “locked” for editing</td>
</tr>
<tr>
<td>Flexible Authorization</td>
<td>• Role-based approval (“four eyes” principle)  &lt;br&gt; • Self-approval  &lt;br&gt; • Emergency bypass (requires password)</td>
</tr>
<tr>
<td>Policy Installation</td>
<td>• Only approved policies can be installed  &lt;br&gt; • Installation email notification</td>
</tr>
<tr>
<td>Highlighting</td>
<td>• Changes highlighted in Check Point SmartDashboard  &lt;br&gt; • List of changes in SmartDashboard</td>
</tr>
<tr>
<td>Reports</td>
<td>• Report of session changes in HTML format  &lt;br&gt; • Reports can be saved/emailed/printed</td>
</tr>
<tr>
<td>Session Information Tracking</td>
<td>• Session information pane with session info, notes and list of changes  &lt;br&gt; • Review changes in sequential order</td>
</tr>
<tr>
<td>Session Tracking</td>
<td>• View all sessions created  &lt;br&gt; • View session changes  &lt;br&gt; • View session status (pending, approved, rejected, etc.)</td>
</tr>
<tr>
<td>Session Comparison</td>
<td>• Compare changes between different sessions  &lt;br&gt; • Compare changes between installed session and an approved session</td>
</tr>
<tr>
<td>Comprehensive Auditing</td>
<td>• Every step in session is logged (session creation, submission, approval/rejection, installation)  &lt;br&gt; • Every change created within a session generates an audit log  &lt;br&gt; • All session audit logs have a session ID for session filtering  &lt;br&gt; • All session audit logs contain change description: old/new value, session information, admin information  &lt;br&gt; • Session audit logs are sent to Check Point SmartView Tracker  &lt;br&gt; • All changes to objects generate an audit log  &lt;br&gt; • All changes to rules generate an audit log</td>
</tr>
<tr>
<td>Check Point Management Integration</td>
<td>• Seamless integration with Check Point Network Policy Management  &lt;br&gt; • Check Point Multi-Domain Security Management (Provider-1) support  &lt;br&gt; • Track changes for CMAs  &lt;br&gt; • Track changes on global policy</td>
</tr>
<tr>
<td>Internet Protocol Version</td>
<td>• IPv6 and IPv4</td>
</tr>
</tbody>
</table>