Check Point® SOFTWARE TECHNOLOGIES LTD.

SmartWorkflow Software Blade

SmartWorkflow
Edit Policies
Review Changes
Approve Changes
Audit Changes
SmartWorkflow Software Blade
SmartWorkflow
Logging & Status
IPS
Management Portal
User Directory
IPS Event Analysis
SmartProvisioning

Overview

SmartWorkflow provides a formal process of policy change management that helps administrators reduce errors and enhance compliance. Changing business needs produce a constant stream of requests to change firewall security policies. These changes can have far reaching implications if not done correctly including: slower firewall performance, network downtime, increased security risks, and lack of compliance with corporate and industry standards. Enterprises that have multiple firewall administrators and an environment of frequent changes need an automated solution that helps them review and authorize policy changes against approved configuration standards. Check Point's SmartWorkflow software blade automates policy change management with visual traceability and full auditability.

Key Benefits

- Enforces a formal process of tracking, approving and auditing security policy changes
- Streamlines change management increasing operational efficiency
- Reduces errors by providing granular visibility into policy changes
- Aligns to an organizations existing change management approval process
- Enhances compliance through audit trails and built-in role segregation
- One-stop, total policy lifecycle management

Features

- Automated change management
- Easy visualization of changes

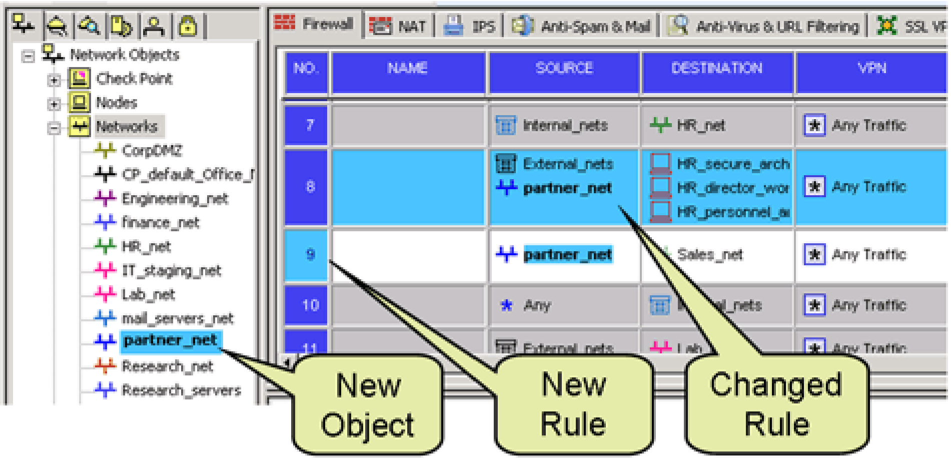
- Session Approval
- Policy revisions and baseline comparisons
- Audit Trails

Automated change management

Administrators have a constant need to make firewall changes. These changes are often done manually and hurriedly resulting in mis-configurations and duplication of rules. Check Point's SmartWorkflow helps administrators track changes to the rule bases, network objects, security policies, users, administrators, groups, OPSEC applications, VPN communities and servers. Changes are tracked in entities called *sessions* which are logical units that contain a set of changes made within SmartDashboard.

Easy visualization of changes

Changes made to rules and objects are highlighted in SmartDashboard.



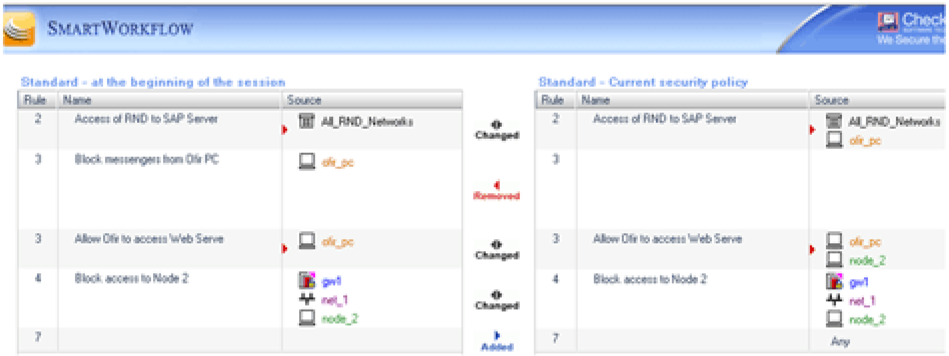
Firewall | NAT | IPS | Anti-Spam & Mail | Anti-Virus & URL Filtering | SSL VP

- Network Objects
  - Check Point
  - Nodes
  - Networks
    - CorpDMZ
    - CP_default_Office_
    - Engineering_net
    - finance_net
    - HR_net
    - IT_staging_net
    - Lab_net
    - mail_servers_net
    - partner_net
    - Research_net
    - Research_servers

NO.	NAME	SOURCE	DESTINATION	VPN
7		Internal_nets	HR_net	Any Traffic
8		External_nets partner_net	HR_secure_arch HR_director_wor HR_personnel_a	Any Traffic
9		partner_net	Sales_net	Any Traffic
10		Any	[illegible]l_nets	Any Traffic
11		External_nets	Lab	Any Traffic

Figure 1: Easy visualization of changes made to rule-base

Administrators can also 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 changed, who changed it, as well as the previous time it was modified and by whom. This enables the administrator to easily review the changes and their impact on the entire rule-base.



Standard - at the beginning of the session

Rule	Name	Source
2	Access of RND to SAP Server	All_RND_Networks
3	Block messengers from Ofir PC	ofir_pc
3	Allow Ofir to access Web Serve	ofir_pc
4	Block access to Node 2	gw1 net_1 node_2
7		

Changed
Removed
Changed
Changed
Added

Standard - Current security policy

Rule	Name	Source
2	Access of RND to SAP Server	All_RND_Networks ofir_pc
3		
3	Allow Ofir to access Web Serve	ofir_pc node_2
4	Block access to Node 2	gw1 net_1 node_2
7		Any

Figure 2: Policy Change Summary Report

Session Approval

SmartWorkflow adds an extra layer of security by ensuring that a changed security policy cannot be installed without a manager's approval (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, the administrator can approve his own changes, or in case of an emergency, a policy can be installed without official approval with the appropriate password.

Policy revisions and baseline comparisons
Prior to approving a session a manager can review the Security Configuration Change Summary Report which provides a summary of the objects added, changed or deleted and how those changes compare to the currently installed Security Policy. In addition, they can review the changes between any two sessions or they can view changes of a single session within SmartDashboard in "read-only" mode.

Audit Trails
Workflow 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 Smartview Tracker as audit logs.

Specifications

Feature	Detail
Session based policy changes	• Security policy changes are done in the context of a session • Notes can be added to sessions for clarification • Changes made within a session can be discarded • Sessions submitted for approval are "locked" for editing
Flexible Authorization	• Role-based approval (four eyes principle) • Self-approval • Emergency bypass (requires password)
Policy Installation	• Only approved policies can be installed • Installation email notification
Highlighting	• Changes highlighted in SmartDashboard • List of changes in SmartDashboard
Reports	• Session changes report in HTML format • Reports can be saved/emailed/printed
Session information tracking	• Session information pane with session info, notes and list of changes • Review changes in sequential order
Sessions tracking	• View all sessions created • View session changes • View session status (pending, approved, rejected etc.)
Sessions comparison	• Compare changes between different sessions • Compare changes between installed session and an approved session
Comprehensive Auditing	• Every step in session is logged (session creation, submission, approval/rejection, installation) • Every change created within a session generates an audit log • All session audit logs have a session ID for session filtering • All session audit logs contain change description

	(old/new value) + session info + admin info • Session audit logs are sent to SmartView Tracker • All changes to objects generate an audit log • All changes to rules generate an audit log
Check Point Management integration	• Seamless integration with SmartCenter • Provider-1 support o Track changes for CMAs o Track changes on global policy

Support

Check Point offers a range of support programs for customers using our software and hardware products.

Support Programs
Choose from either direct Enterprise Based Support from Check Point or Collaborative Enterprise Support from our certified partners. Please visit our Support Programs and Plans for detailed information or Compare Programs for a summary of features.

Check Point offers support online, by phone and onsite directly or via its network of partners. Open a ticket online anytime with Check Point Support via Check Point User Center.

Check Point Professional Services are an essential component in successfully deploying, upgrading, and optimizing your Check Point products for maximum security and benefits. Check Point will assign a primary consultant who will serve as the single point of contact and perform the majority of the activities associated with your service needs.

Check Point Training and Certification provides the critical knowledge and skills to maximize security and ROI from Check Point solutions. Please visit the course catalog for a list of classes.

Check Point Appliance Support programs provide technical support, software updates and upgrades, and the replacement of faulty hardware.

Check Point Enterprise Support Lifecycle Policy
Check Point Enterprise Support Lifecycle Policy outlines the product support guidelines for a product's lifecycle. The objective of this policy is to standardize and normalize product lifecycle practices, enabling Check Point customers to make informed purchase, support and upgrade decisions.

Check Point is committed to providing support for all software products for a minimum of four (4) years, starting from the general availability date of the product's major version. 'General availability date' is defined as the date on which a product is officially made available for purchase. See the Check Point Enterprise Software Support Timeline

Check Point offers a Software License Agreement & Limited Hardware Warranty for all products. Please see more information about warranty at Hardware Warranty