MAXIMIZE SECURITY

SEGMENT MANAGEMENT INTO MULTIPLE VIRTUAL DOMAINS

Companies of any size face security management challenges when their business spans offices located in several regions or countries. Multiple security gateways, multiple sites requiring different or conflicting security policies and multiple administrators can quickly create a complex security environment. Administrators need the right tools to effectively manage multiple security policies with rules enforcing appropriate user access and preventing attacks. This enables secure communication and fail-over capabilities.

EFFICIENT, SECURE, CONSOLIDATED MANAGEMENT

Check Point Multi-Domain Security Management provides more security and control by segmenting your security management into multiple virtual domains. Any size business can benefit—easily creating virtual domains based on geography, business unit or security functions to strengthen security and simplify management. IT managers can easily deploy Multi-Domain Security Management into their current security environment, simplifying administration and leveraging their existing infrastructure. Organizations can expand their security management at any time, deploying new security domains with a single click.

When complexity or geography complicate management and threaten security, segmenting security into multiple virtual domains can provide dramatic improvements in operational efficiency and better security. Multi-Domain Security Management enables simultaneous, central management of many distinct security policies and consolidation of security hardware. Multi-Domain Management software blades, based on proven technology, help administrators consolidate their security management while preserving the independence of each domain. The Global Policy enforces a common security baseline, while Security Domain Software Blades enable easy creation of new virtual management domains.

BUILT UPON A SCALABLE, EXTENSIBLE ARCHITECTURE

Simplified management and provisioning of security in complex environments

Common security baseline enforced across multiple domains

Increase efficiency through consolidation of security management infrastructure and resources

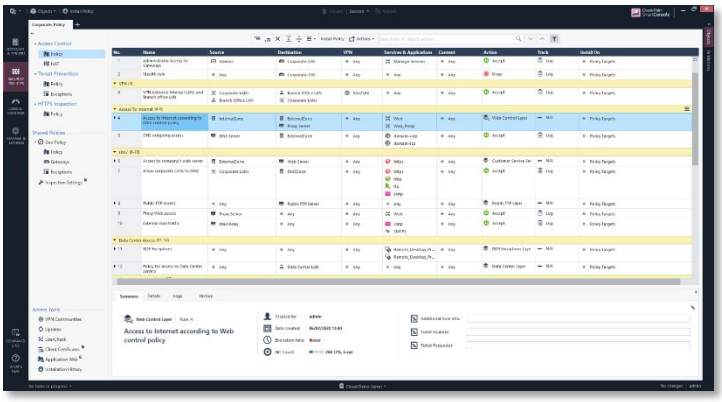
SPOTLIGHT ON MANAGEMENT

Lower the complexity of managing your security

When it comes to security management, Check Point has a solution. From zero-touch gateway provisioning to security policy management to threat visibility and analytics to compliance and reporting to large scale multi-domain management to central deployment of software updates to codifying security management using RESTful APIs – Check Point has you covered.

ONE CONSOLE TO MANAGE THEM ALL

With one console, security teams can manage all aspects of security from policy to threat prevention – across the entire organization – on both physical and virtual environments. Consolidated management means increased operational efficiency.



UNIFIED POLICY

In addition to a unified console, a unified access control policy for users, applications, data and networks simplifies policy management.

NEXT GENERATION POLICY MANAGEMENT

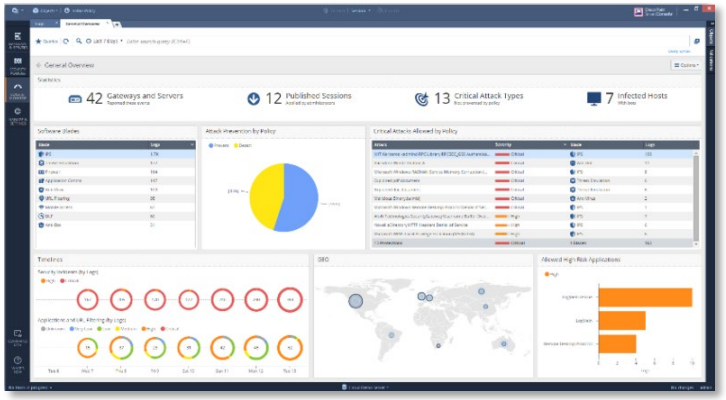
Check Point's next generation policy makes it extremely easy to segment policy into manageable sections with inline shared policies. Create rules in sub-policies aligned to specific business function like control of safe Internet use. Then share it across teams, ensuring consistency.

COLLABORATION

Work without conflict. Check Point's security management software is recognized for superior access control and policy organized in layers and sub-layers. Session-based object locking enables multiple administrators to work simultaneously on the same rule base. Smart-1 Cloud provides two access or permission levels: administrator and read-only.

THREAT MANAGEMENT

Threat Management is fully integrated, with logging, monitoring, event correlation and reporting in one place. Visual dashboards provide full visibility into security across the network, helping you monitor the status of your enforcement points and stay alert to potential threats.



COMPLIANCE REPORTS

Security can be complex, but there are industry and security best practices to guide you. Real-time compliance monitoring and reporting is built-in, showing admins how their policy compares with Security Best Practices and regulations such as GDPR, HIPAA and PCI DSS.

APIS ENABLE OPERATIONAL EFFICIENCY

With too much work and too little staff, security teams need to work smarter. Leverage security management APIs to automate routine and repetitive tasks.

ZERO-TOUCH DEPLOYMENT

An intuitive web-based user interface enables large enterprises to provision security efficiently. Apply a template describing device configuration settings to your inventory of new security gateways. When powered on Check Point gateways get their configuration from the cloud and are ready for a security policy.

SPOTLIGHT ON MULTI-DOMAIN MANAGEMENT

Multi-domain, Multi-policy Management

Segregate complex management environments into multiple domains. Each management domain is an independent security management environment with a separate database, log server and its own set of security policies.

SECURE ARCHITECTURE

Create separate certificate authorities for each management domain and the multi-domain system to ensure secure and private communications between gateways and their management domains, and between management domains and the multi-domain system.

GLOBAL POLICY

Define templates for global security rules and assign them to multiple domains. Global security policy can be assigned to all managed domains or just to a select group of domains.

GRANULAR ADMINISTRATOR CONTROLS

Create and centrally manage multiple administrators for multi-domain management environments. Administrators can be assigned to specific domains.

CENTRALIZED MONITORING

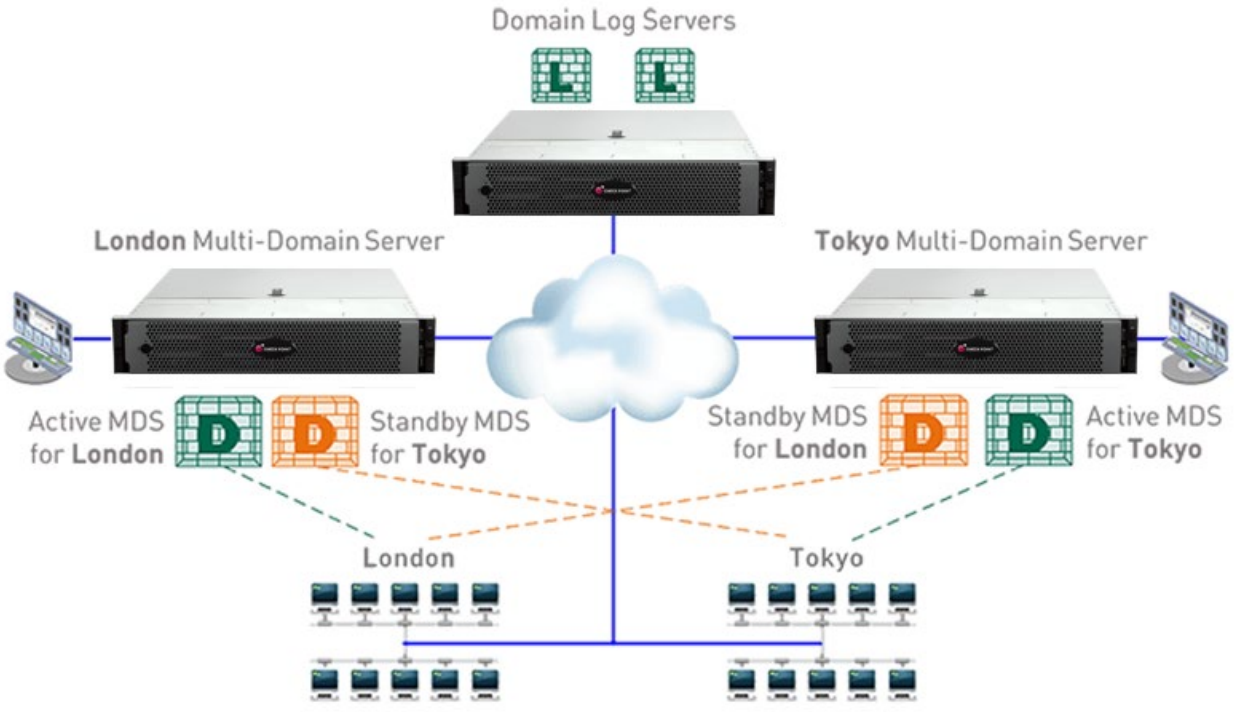
Monitor all multi-domain system components (domains, global policy, administrators, etc.) and gateways from a central location.

DOMAIN INDEPENDENT LOG SERVER

Collect and store security gateway logs for each domain in a separate, independent log server.

REDUNDANCY AND BACKUP

Synchronize multi-domain management databases (MDS database, global policy, and ICA database) between multiple multi-domain servers. Rest assured knowing that your security management is backed up and highly available.



MULTI-DOMAIN SECURITY MANAGEMENT FEATURES

Feature	Details
Multiple Domain-Based Management	Complex management environment can be segregated into multiple management domains. Each management domain is an independent security management environment with a separate database, log server and its own set of security policies.
Multi-Domain Dashboard	Single security console to manage multiple domains. Graphical interface to view, create and manage all management domains. Assign global policy to different management domains. Create and manage administrators and GUI clients.
Distributed Domain Management	Management domains can be distributed across many multi-domain servers.
Global Rules	Define global security rules templates and assign them to virtual domains. Global policy can be assigned to group of management domains.
Global Objects	Centralized configuration and management of shared objects that can be used across multiple domains.
Global VPN Policy	Centralized definition and management of VPN communities across multiple domains.
Global IPS Policy	Centralized definition and management of IPS policies across multiple management domains.
Role-based Access Controls	
Granular Role-Based Administration	Create and centrally manage multiple administrators for multi-domain environments. Assign administrators to specific domains.
Hierarchical Administrator Role Support	Assign administrator rights to manage specific domains and rights and permissions to management different aspects of the multi-domain system.
Multiple Simultaneous Administrator Access	Allows multiple administrators to work on different management domains simultaneously.
Multiple Authentication Methods For Administrators	Multiple authentication methods for administrators using internal certificate authority or external third party systems including RADIUS, TACACS, and RSA.
Monitoring	
Centralized Monitoring of Multi-Domain Systems	Centralized monitoring of all multi-domain system components (domains, global policy, administrators, etc.)
Centralized Monitoring of Managed Gateways	Centralized monitoring of all gateways managed by the multi-domain management system.
Log Management	
Domain Independent Log Server	Each domain has a predefined log server for collection and storage of logs from all security gateways managed by that domain.
Multi-Domain Log Module Support	Optional standalone multi-domain server dedicated to log collection and storage, allowing separation of critical management activities from logging traffic.
Domain for Log Server Support	Optional dedicated domain for log collection and storage, allowing separation of critical domain management activities from logging activities.

MULTI-DOMAIN SECURITY MANAGEMENT FEATURES (continued)

Feature	Details
Redundancy and Backup	
Multi-Domain Server Synchronization	Support synchronization of multi-domain management databases (MDS database, Global Policy and ICA database) between multiple multi-domain servers.
Domain High Availability	Allow synchronization of domain databases between multiple multi-domain servers.
Export/Import of Multi-Domain Systems and Domains	Export/Import entire multi-domain system or a specific domain for maximum backup and recovery options.
Security Management Backup	Backup your virtual management domain to a standard security management system.
Deployment	
Multi-Platform Support	Supported on Smart-1 Security Management Appliances and Open Servers

Smart-1 Security Management Appliances

	Smart-1 6000-L	Smart-1 6000-XL
Managed Gateways (base/plus models)	75/150	200/400
Maximum Domains	50	200

Multi-domain Security Management Open Server Requirements

Component	GAiA
CPU	Intel Pentium IV, 2.6 GHz or equivalent
Memory	32 GB minimum, maximum supported memory is 512 GB
Recommended Free Disk Space	1 TB
Minimum Free Disk Space	100 GB for the Multi-Domain Server, 110 GB for each additional Domain

ORDERING QUANTUM MANAGEMENT

Smart-1 Appliances[1]	SKU
Smart-1 6000-L	
Smart-1 6000-L Base Multi-Log appliance for 75 gateways and 10 domains (perpetual), 96 GB RAM, 24 TB HDD, 2x AC PSUs, LOM	CPAP-NGSM6000L-BASE-MLOG-10
Smart-1 6000-L Plus Multi-Log appliance for 150 gateways and 10 domains (perpetual), 192 GB RAM, 24 TB HDD, 2x AC PSUs, LOM	CPAP-NGSM6000L-PLUS-MLOG-10
Smart-1 6000-XL	
Smart-1 6000-XL Base Multi-Log appliance for 200 Gateways and 10 domains (perpetual), 192 GB RAM, 6x 4TB SSD, 2x AC PSUs, LOM	CPAP-NGSM6000XL-BASE-MLOG10
Smart-1 6000-XL Plus Multi-Log appliance for 400 gateways and 10 domains (perpetual), 384 GB RAM, 6x 4TB SSD, 2x AC PSUs, LOM	CPAP-NGSM6000XL-PLUS-MLOG10

1 the Smart-1 6000-L supports up to 50 domains, the Smart-1 6000-XL supports a maximum of 200 domains.

ORDERING QUANTUM MANAGEMENT (continued)

Open Server Management Software Products	SKU
Next Generation Security Management Software Multi-domain for 150 gateways and 5 domains (SmartEvent & Compliance 1 year)	CPSM-NGSM150-MD5
Next Generation Security Management Multi-Log Manager software for 150 gateways and 10 domains (perpetual)	CPSM-NGSM150-MLOG10
Next Generation Security Management Software Multi-domain for 50 gateways and 5 domains (SmartEvent & Compliance 1 year)	CPSM-NGSM50-MD5
Next Generation Security Management Multi-Log Manager software for 50 gateways and 10 domains (perpetual)	CPSM-NGSM50-MLOG10
Next Generation Security Management Software Multi-domain for 25 gateways and 5 domains (SmartEvent & Compliance 1 year)	CPSM-NGSM25-MD5

Additional Domain Extensions [1]	SKU
5 domains package for Multi-domain Security Management	CPSB-DMN-5
10 domains package for Multi-domain Security Management	CPSB-DMN-10
25 domains package for Multi-domain Security Management	CPSB-DMN-25
50 domains package for Multi-domain Security Management	CPSB-DMN-50
100 domains package for Multi-domain Security Management	CPSB-DMN-100

1 additional domain packages are additive.