



Check Point Software Technologies

Correlation with NIST Special Publication 800-41, Revision 1,  
“Guidelines on Firewalls and Firewall Policy”  
summaries of recommendations.

## Table of contents:

- Page 1: Executive summary
- Page 2: NIST 800-41 Revision 1 Section 2.4  
Overview of Firewall Technologies, Summary of Recommendations  
*~ The use of NAT should be considered a form of routing, not a type of firewall.*
- Page 3: *~ Organizations should only permit outbound traffic that uses the source IP addresses in use by the organization.*
- Page 4: *~ Compliance checking is only useful in a firewall when it can block communication that can be harmful to protected systems.*
- Page 5: *~ When choosing the type of firewall to deploy, it is important to decide whether the firewall needs to act as an application proxy.*
- Page 6: *~ Management of personal firewalls should be centralized to help efficiently create, distribute, and enforce policies for all users and groups.*
- Page 7: NIST 800-41 Revision 1 Section 3.4  
Firewalls and Network Architectures, Summary of Recommendations
- Page 8: *~ Different common network architectures lead to very different choices for where to place a firewall, so an organization should assess which architecture works best for its security goals.*
- Page 9: *~ If an edge firewall has a DMZ, consider which outward-facing services should be run from the DMZ and which should remain on the inside network.*  
*~ Do not rely on NATs to provide the benefits of firewalls.*  
*~ In some environments, putting one firewall behind another may lead to a desired security goal, but in general such multiple layers of firewalls can be troublesome.*
- Page 10: NIST 800-41 Revision 1 Section 4.5 Firewall Policy, Summary of Recommendations  
*~ An organization's firewall policy should be based on a comprehensive risk analysis.*
- Page 11: *~ Firewall policies should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic.*
- Page 12: *~ Policies should take into account the source and destination of the traffic in addition to the content.*
- Page 13: *~ Many types of IPv4 traffic, such as that with invalid or private addresses, should be blocked by default.*
- Page 14: *~ Organizations should have policies for handling incoming and outgoing IPv6 traffic.*
- Page 15: *~ An organization should determine which applications may send traffic into or out of its network and make firewall policies to block traffic for other applications.*
- Page 16: NIST 800-41 Revision 1 Section 5.2.2 Policy Configuration
- Page 19: NIST 800-41 Revision 1 Section 5.2.3 Logging and Alerts Configuration
- Page 23: NIST 800-41 Revision 1 Section 5.5 Management
- Page 25: Conclusion

## Executive Summary

This guide is intended to serve as a collection of general guidelines and principles that, if followed, will help to improve your company's security posture. Please note that both the NIST guidelines and the vendor's best practices are generic in nature, and that there are no universal solutions when it comes to securing a particular infrastructure.

This document is based on NIST Special Publication 800-41 Revision 1, (Guidelines on Firewalls and Firewall Policy), Check Point Software Technologies LTD. R77.X feature highlights and specific administration recommendations.

Check Point R77.X represents a comprehensive suite of infrastructure security solutions. They are comprised of dedicated hardware devices, virtual appliances and software components called "blades", each representing certain functionality. There are management and security blades that are designed to cover most aspects of information technology security.

Although Check Point products could be deployed on a variety of operating systems, the preferred is the proprietary Gaia OS, created as a culmination of efforts in combining the best features of Nokia IPSO with those of Check Point Secure Platform. The Gaia OS is a purpose-build hardened operating system based on Linux. Particular steps taken by Check Point for the OS hardening could be found in the [CP R77 Gaia Hardening Guide.pdf](#) and are available for download on the UserCenter portal.

As we follow NIST SP 800-41 Revision 1, various Check Point blades will be mapped to the summaries of recommendations provided therein. In your case, some of the functionality described will likely be delegated to the devices, software or services by vendors other than Check Point, (i.e. VPN endpoint devices, client security, data loss prevention, etc.). In those cases, you should consider how the third-party solutions integrate with your Check Point security infrastructure components in order to maximize your effective coverage.

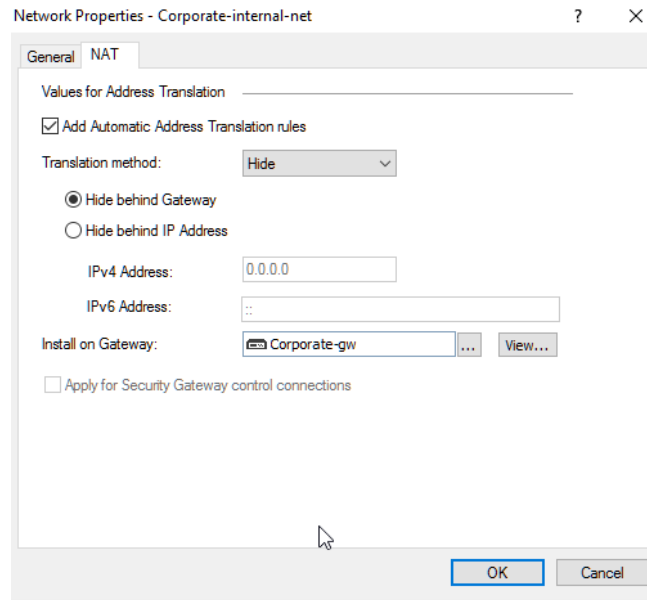
Check Point Compliance blade could be utilized to automatically verify your configurations' ongoing adherence to the NIST SP 800-41 Revision 1, as well as a number of other standards, such as PCI DSS or ISO 27002, and to unambiguously highlight non-compliant systems and lapses in regulatory requirements.

You can use the Compliance blade in the trial mode during initial stages of your security infrastructure deployment and, should you find it useful, the blade could be licensed at a later date allowing your administrators to easily spot deviations from policies required by regulations you are subjected to.

## NIST 800-41 Revision 1 Section 2.4 Overview of Firewall Technologies, Summary of Recommendations

- *The use of NAT should be considered a form of routing, not a type of firewall.*

Check Point firewalls not deployed in a transparent bridge mode are capable of routing as well as NAT and PAT traffic manipulation. While masquerading does help in reducing exposure of address ranges susceptible to attacks, it is a task executed by the routing daemon of the firewalls. NAT could be defined either by enabling it in the properties of the objects,

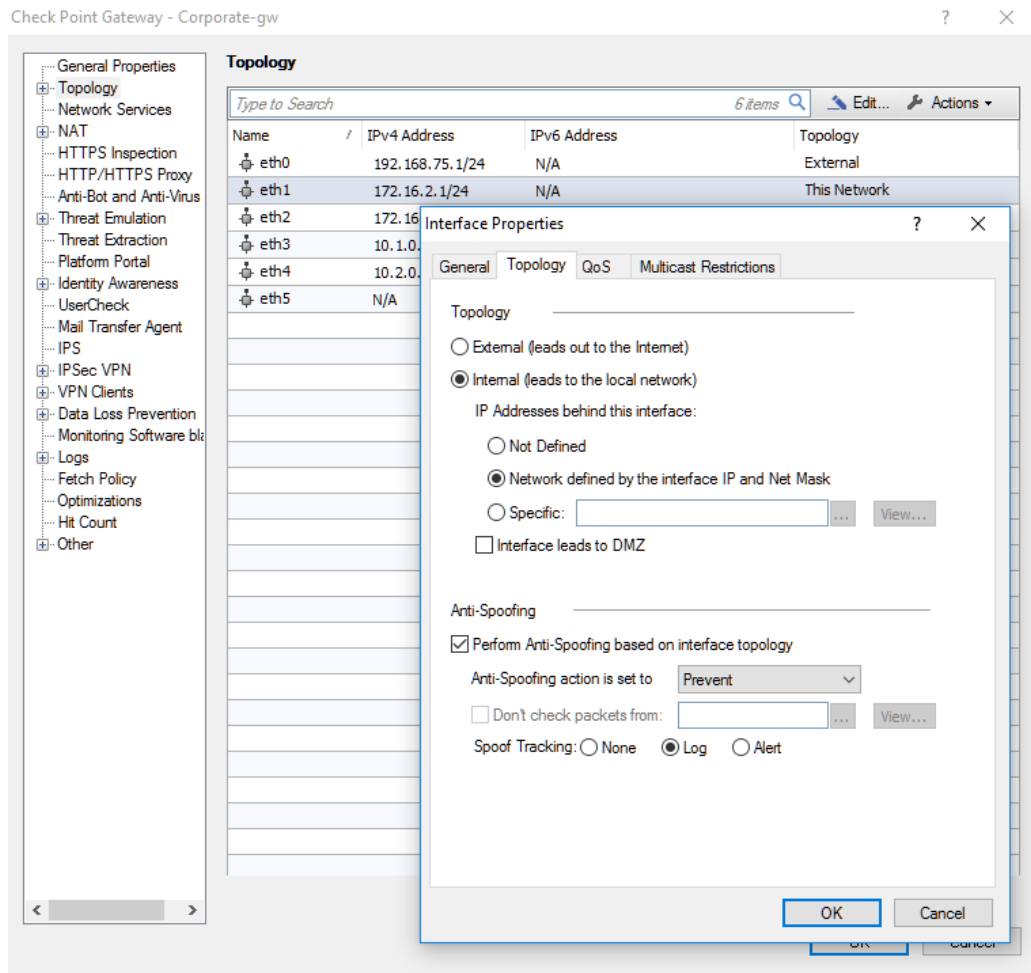


in which case the NAT rule will be created automatically, (e.g. Rules No. 2-6 below), or by manually creating NAT rules in the Smart Dashboard\Firewall\NAT policy, (e.g. Rule No. 1):

No.	Original Packet			Translated Packet			Install On	Comment
	Source	Destination	Service	Source	Destination	Service		
1	SMTPServer	Any	smtp	NAT_device1	Original	Original	Corporate-gw	Manual NAT rule for SMTP
Automatic Address Translation Rules (Rules 2-28)								
2	Corporate-WA-	Any	Any	Corporate-WA-	Original	Original	All	Automatic rule (see the network object data).
3	Any	Corporate-WA-	Any	Original	Corporate-WA-	Original	All	Automatic rule (see the network object data).
4	Corporate-mail	Any	Any	Corporate-mail	Original	Original	All	Automatic rule (see the network object data).
5	Any	Corporate-mail	Any	Original	Corporate-mail	Original	All	Automatic rule (see the network object data).
6	Remote-1-web-	Any	Any	Remote-1-web-	Original	Original	Remote-1-gw	Automatic rule (see the network object data).

- Organizations should only permit outbound traffic that uses the source IP addresses in use by the organization.

Check Point firewalls are capable of enforcing Anti-Spoofing on all of their interfaces. Only IP addresses that are either tied to topology of the interfaces or are manually defined could traverse the firewall:

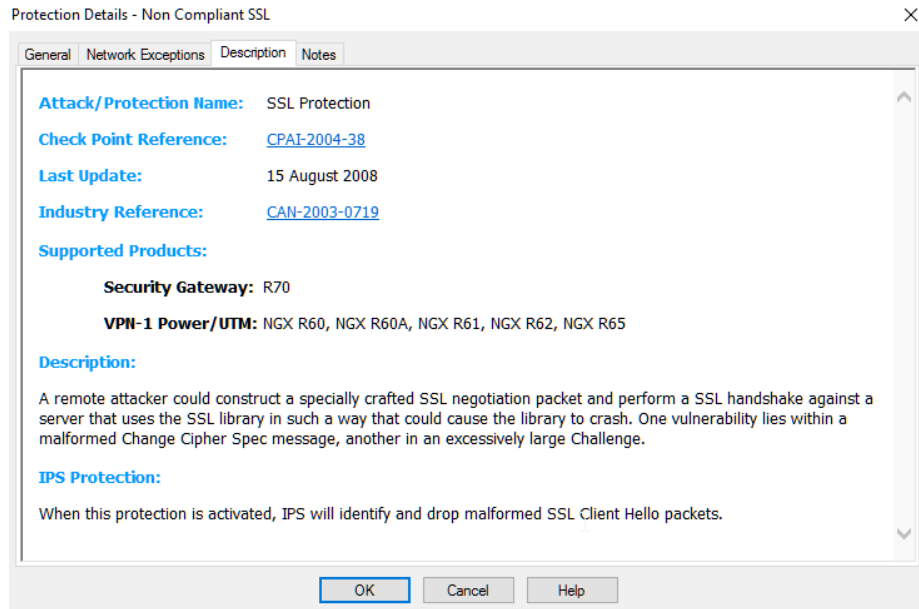


If the interface in question is expected to accept traffic not only from the network to which it belongs, exit this menu, create a group object containing all other objects that should be allowed to traverse firewall from this interface, return to this menu and check the radio button “Specific”, then browse to the group object created earlier and choose it to populate the box.

For clarification about the function of the “Interface leads to DMZ” checkbox and to see what policies and protections are available for the DMZ designated interfaces, see [sk108057](#).

- *Compliance checking is only useful in a firewall when it can block communication that can be harmful to protected systems.*

Check Point IPS blade is capable of this function. Found in **Smart Dashboard\IPS\Protections\By Type \Protocol Anomalies**, particular violation actions are either already set to “protect,” or could be enabled in either one of two policies created by default, or in a new policy that could be created from scratch, or by cloning a pre-existing one. See the example below for protection against a Non-Compliant SSL:



It is fairly common for some of the modern useful applications to be out of compliance with RFCs. Should this be an issue with some of the valid and expected traffic, you have the ability to define exceptions under the “**Network Exceptions**” tab of a particular protection.

- When choosing the type of firewall to deploy, it is important to decide whether the firewall needs to act as an application proxy.

Check Point firewalls could act in the capacity of HTTP/HTTPS proxies (see sk110348), as well as serving as MTAs and filters for the email traffic. Shown here is the “Anti-SPAM and Mail” overview page with nested links to settings of its components:

Enforcing Gateways		Database Updates	
Traditional Anti-Virus	5/15 Gateways	Anti-Spam	4/21 Gateways
		Configure	Automatic updates are not configured
Some Anti-Spam Mail features involve communication with an external server. For more information, refer to our <a href="#">privacy policy</a> .			
	<b>Content based Anti-Spam</b> Filter spam based on content fingerprint	High protection	<ul style="list-style-type: none"> <li>Filter spam</li> <li>Filter suspected spam</li> </ul> <ul style="list-style-type: none"> <li>Protects against all types of spam</li> <li>Filters more than 97% of spam</li> <li>A false positive rate of 1 in a 100,000</li> <li>Up to thousands of messages/sec</li> </ul>
	<b>IP Reputation Anti-Spam</b> Filter spam from known spammers	High protection	<ul style="list-style-type: none"> <li>Filter spam</li> <li>Filter suspected spam</li> </ul> <ul style="list-style-type: none"> <li>Blocks the majority of malicious mail</li> <li>Filters more than 70% of spam</li> <li>Saves bandwidth. Improves performance</li> </ul>
	<b>Block List Anti-Spam</b> User defined IPs and addresses blocking	Block	<ul style="list-style-type: none"> <li>Block senders by IP</li> <li>Block senders by address</li> </ul> <ul style="list-style-type: none"> <li>0 IPs will be blocked</li> <li>0 Senders/Domains will be blocked</li> </ul>
	<b>Mail Anti-Virus</b> Scan and filter mail for malware	Block	<ul style="list-style-type: none"> <li>Block</li> <li>To enable on UTM-1 Edge go to Anti-Virus Settings</li> </ul> <ul style="list-style-type: none"> <li>Up to thousands of messages/sec</li> </ul>
	<b>Zero hour malware protection</b> Filter mail using rapid response signatures	Block	<ul style="list-style-type: none"> <li>Block</li> <li>Performance Impact</li> </ul> <ul style="list-style-type: none"> <li>Immediate proactive malware protection</li> <li>Up to thousands of messages/sec</li> </ul>
	<b>IPS</b> Email IPS protections	Go to IPS Tab to manage IPS profiles IPS mail	<ul style="list-style-type: none"> <li>3 POP3 servers defined</li> <li>3 SMTP servers defined</li> <li>3 IMAP servers defined</li> </ul>

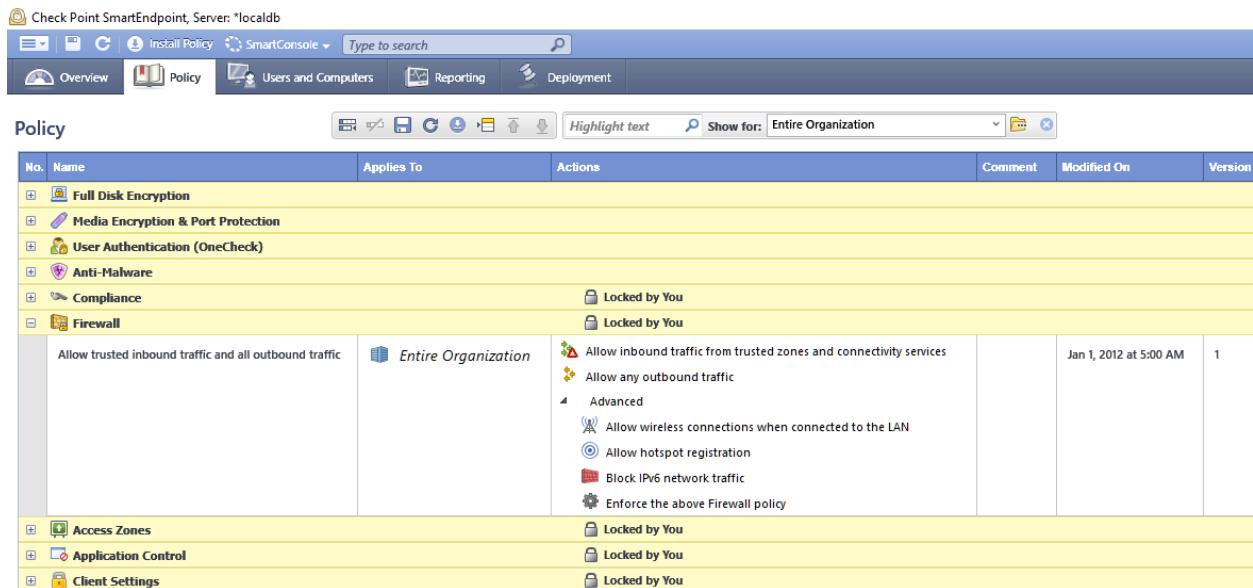
Security functions are performed by “IPS”, “Threat Prevention” and “Anti-SPAM and Mail” blades.

Even if these functions are sufficient for your purposes, you will be better served by using third party, custom built application proxies with extended functionalities by forwarding identified traffic to external appliances.

- *Management of personal firewalls should be centralized to help efficiently create, distribute, and enforce policies for all users and groups.*

Check Point SmartEndpoint Server allows for centralized management of personal firewalls. NIST defines personal firewalls as a “software that runs on a desktop or laptop PC with a user-focused operating system such as Microsoft Windows or Mac OS X”.

Check Point endpoint security solutions include data security, network security, advanced threat prevention, forensics and remote access VPN for complete endpoint protection. To simplify security administration, the endpoint suite products can be managed using a single console:



Please note that when using centralized endpoint security blades, your tradeoff is the speed of deployment of new OS versions or service packs, as typically the security vendors tend to trail OS vendors by a few months to confirm stability of their solutions. This does not affect deployment or installation of regular security patches for OS, or software installed on the endpoints.

Given the interdependency between OS and the Endpoint Security Client blades, it is prudent to define control groups to test the application of endpoint policies in order to verify their functionality before distribution to the intended scope of desktops and laptops.

Same is applicable to the installation of security patches and updates for the operating systems in order to assure that there is no negative impact on functionality of the Endpoint Security Client software blades.



## NIST 800-41 Revision 1 Section 3.4 Firewalls and Network Architectures, Summary of Recommendations

- *In general, a firewall should fit into a current network's layout. However, an organization might change its network architecture at the same time as it deploys a firewall as part of an overall security upgrade.*

If need be, Check Point firewall could be deployed in the “Bridge Mode”, acting as a two-port switch that belongs to the same broadcast domain. These blades are supported in the Bridge Mode when used on either physical or virtual systems:

Supported Blade	Supports Gateways in Bridge Mode	Supports Virtual Systems in Bridge Mode
Firewall	Yes	Yes
IPS	Yes	Yes
URL Filtering	Yes	Yes
DLP	Yes	No
Anti-Bot and Anti-Virus	Yes	Yes
Application Control	Yes	Yes
HTTPS Inspection	Yes	No
Identity Awareness	Yes	No
Threat Emulation	Yes	Yes
QoS	Yes	No
Client Authentication	No	No
User Authentication	No	No

You can use any two of the interfaces, either physical or VLAN, in order to accommodate this configuration. This option is valuable if you are trying to implement security functions described above in the existing network without changing your routing schema on certain production segments of your network.

It is important to note that you can use the same firewall appliance or cluster for both the routed and Bridge Mode implementations at the same time.

A newly designed infrastructure, or one undergoing modification, is better served by creating network segmentation and thus should rely on routed firewall implementation strategies.

Check Point physical and virtual appliances support static and dynamic routing, as well as policy-based routing, allowing for flexibility of conditional traffic flow manipulation.

Please note that dynamic routing should be used with extreme care, as routing changes propagated from one of the network segments may inadvertently affect the functionality of all other segments dependent on the firewall. Additionally, dynamic routing coupled with loosely defined Anti-Spoofing and Security Policy rules may result in sensitive data being redirected to unintended destinations.

- *Different common network architectures lead to very different choices for where to place a firewall, so an organization should assess which architecture works best for its security goals.*

Traditionally implemented at the perimeter, firewalls are now increasingly required to protect internal network segments, virtual and cloud-based components of hybrid infrastructures.

Due to proliferation of laterally propagated threats (such as ransomware), any single broadcast domain could be exposed. While there are Network Intrusion Prevention systems available to address this type of attacks, they are outside of the scope of this document.

To mitigate the impact of laterally propagating attacks by using Check Point firewalls, one of the following two approaches may be implemented:

1. If the broadcast domain is served by multiple distribution switches, use Bridge Mode deployment to pass the traffic from core to the distribution switches through a firewall equipped with Check Point Antivirus and Threat Prevention components enabled. It would make sense to distribute endpoint connections to the switches serving same broadcast domain in such a way, that members of same departments or hosts serving same application are connected to different switches.
2. Assign endpoints that belong to each department or hosts serving same application to two or more broadcast domains and route them through the firewall with Check Point Antivirus and Threat Prevention components enabled.

VMware VSX simplifies these approaches as it allows for the spawning of multiple fully capable firewall instances on shared hardware with each configured to provide highly-tuned protection to the hosts behind them.

Virtualization and cloud solutions are increasingly taking advantage of the distributed network overlays that create virtual networking environments on top of the existing switching and routing hardware. Commonly referred to as SDN (Software Defined Network), this technology is designed to help organizations take advantage of automation and simplify the scalability of infrastructure.

From a security point of view, this represents challenges related to the fact that the virtual network overlay is invisible to conventional firewalls, as VXLAN traffic is tunneled through those. Not long after this technology has taken hold, security vendors have responded with solutions tailored to address the requirements of massively scalable virtual infrastructures.

Check Point vSEC\* for VMware NSX, AWS and Azure, is designed to integrate with on premise or cloud offerings and, when combined with micro-segmentation, provides the same level of security to virtual and cloud environments as do conventional firewalls to the traditional hardware-centric deployments.\*\*

Additional benefit of employing vSEC is that common security policies could be applied to the instances protecting physical and virtual infrastructures, ensuring adherence to the corporate security standards and a consistent logging format. This allows for simplified troubleshooting and better decision making by security administrators.

\*[Check Point vSEC](#)

\*\*[VMware Micro-Segmentation overview](#)

- *If an edge firewall has a DMZ, consider which outward-facing services should be run from the DMZ and which should remain on the inside network.*

Depending on your firm's overall security stance, you may choose to place application (reverse) proxies in the DMZ and to enable filtering on both ingress and egress traffic. In this case, the outward-facing services are going to be located on the "inside" of the firewall. This solution introduces one more hurdle for attackers to overcome. Some of the application proxies are capable of decrypting the traffic secured by the SSL/TLS encryption. If such a proxy is implemented, its egress traffic could be subjected to the IPS/IDS, antivirus and threat detection analysis that otherwise would not be possible.

Additionally, if a third-party VPN solution is being utilized, the VPN endpoint appliance could be placed in DMZ as well, for similar purposes: the IPSEC or SSL VPN traffic, normally encapsulated, will be decoded and visibility of the security solution analyzing it will be increased. Note that whenever traffic traversing VPN is protected by SSL/TLS encryption, its payload is still hidden from the firewall's threat prevention components.

To achieve maximum visibility into the traffic traversing the firewalls while at the same time not overloading it with processing intensive decryption tasks, use application proxies with SSL/TLS decoding capability and VPN endpoints in the DMZ loops, (one firewall interface in DMZ and one on the inside), outbound SSL/TLS visibility appliances on the inside loops and outward looking servers on dedicated inside zones. This, with the rules permitting traffic to and from devices behind various interfaces of the firewall(s) to appropriate destinations on dedicated ports, will maximize the efficiency of processing and provide excellent visibility and logging depth.

- *Do not rely on NATs to provide the benefits of firewalls.*

See Page 2, "*The use of NAT should be considered a form of routing, not a type of firewall.*"

- *In some environments, putting one firewall behind another may lead to a desired security goal, but in general such multiple layers of firewalls can be troublesome.*

Utilization of multiple layers of firewalls is largely unavoidable in the highly virtualized dynamic environments where solutions such as vSEC or other virtualization firewalls are implemented, or where the networks are heavily segmented to increase the overall security posture. When executed with forethought, including provisions for future expansions, alterations and increase in traffic volume, it is presently the desired approach. Case in point would be a peripheral firewall, (or cluster), with relatively simple rule-base designed to effectively route high volumes of filtered inbound traffic to a second tier of the firewalls, each configured to provide specific protections to particular applications. This second tier of firewalls will perform the heavy lifting of IDS/IPS, antivirus, etc. and hand the processed traffic over to the vSEC instances running on virtual infrastructure.

## NIST 800-41 Revision 1 Section 4.5 Firewall Policy, Summary of Recommendations

- *An organization's firewall policy should be based on a comprehensive risk analysis.*

An ongoing process of risk analysis and remediation should be implemented to allow for continuous assessment of threats and vulnerabilities, existing countermeasures available for mitigation, and the impact caused by compromised systems or data.

Well documented, frequently reviewed and updated firewall policies should be reflective of emerging new threats, discovered vulnerabilities and changing requirements of organization's networks and applications.

Risk analysis is outside of the scope of this document. [NIST Special Publication 800-30 Revision 1](#) could be used to develop an organization-specific risk management policy.

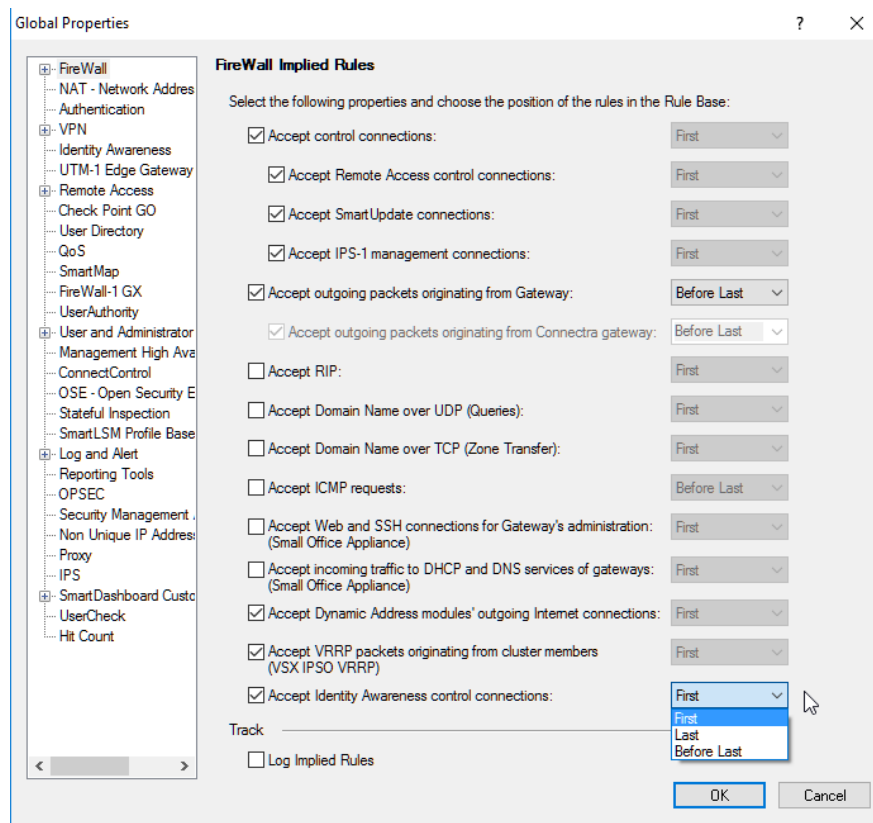
- *Firewall policies should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic.*

Check Point firewalls are, by default, configured to “Deny All” but the traffic defined in “Implied” and “Explicit” rules.

Implied rules are those that take under consideration, for example, routing protocols or secure control connections necessary for remote administration. These could be found in “Global Properties\Firewall”. You have the ability to disable all of the implied rules and to replace them with your own explicit rules within the policy.

Note that the traffic matching implied rules is **not logged** by default. However, you have the ability to enable logging for either all of the implied rules, (by checking “Log Implied Rules” checkbox in “Global Properties\Firewall”), or for select ones (by creating redundant explicit rules with logging or alerting options enabled).

Additionally, some of the “FireWall Implied Rules” have properties pertinent to their position in the rule base. Available parameters are “First”, “Before Last” and “Last” and generally should remain on default settings, unless there is a compelling reason for change.



To make the “FireWall Implied Rules” visible within the policy, click the “View” menu in the SmartDashboard and select “Implied Rules”.

- Policies should take into account the source and destination of the traffic in addition to the content.

For all practical purposes, the majority of your firewall policies is comprised of “Explicit” rules.

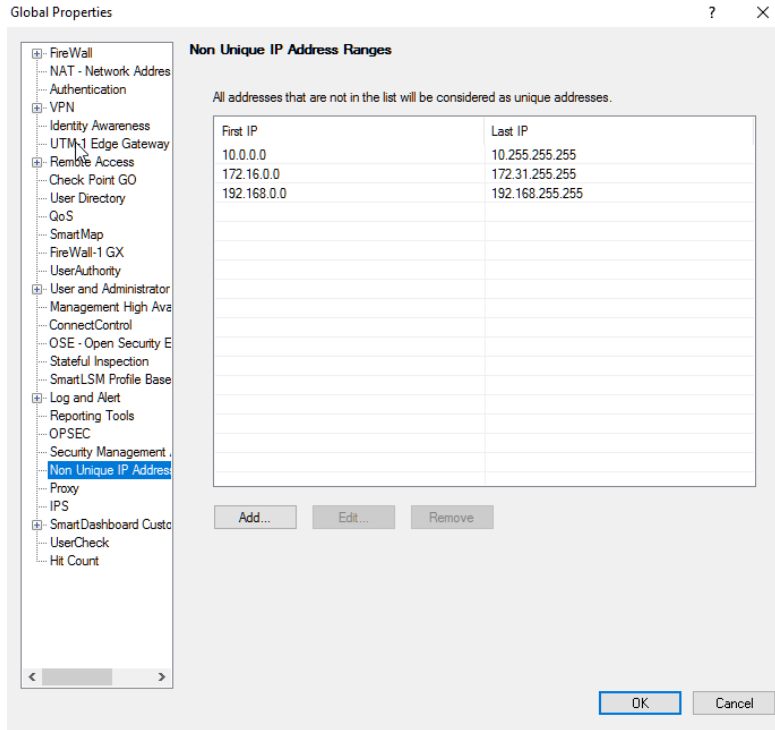
“Explicit” rules are those that you have manually created in the firewall policies. They are highly flexible entities designed to either permit or deny a variety of traffic matching sources, destinations, services, ports, users’ identities, etc., as shown here:

No	Policy	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
Limit Access to Gateways Rule (Rule 1)										
1	2M	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any
VPN Access Rules (Rules 2-5)										
2	514K	Site to site VPN	Any	Any	All_GwToGw	CIFS ftp-port http https smtp	accept	Log	Policy Targets	Any
3	33K	Remote access	Mobile-vpn-user@Any	Any	RemoteAccess	CIFS http https imap	accept	Log	Policy Targets	Any
4	415K	Clientless VPN	Clientless-vpn-user@Any	Corporate-WA	Any Traffic	https	User Auth	Log	Policy Targets	Any
5	3K	Web server	L2TP-vpn-user@Any Customers@Any	Remote-1-web	Any Traffic	http	accept	Log	Policy Targets	Any
Rules for Specific Sites (Rules 6-8)										
6	34K	Outbound HTTP	Remote-2-internal	Any	Any Traffic	http	Client Auth	Log	Remote-2-gw	Any
7	0	Critical subnet	Corporate-internal-net	Corporate-fina Corporate-hr-n Corporate-rnd	Any Traffic	Any	accept	Log	Corporate-gw	Any
8	7M	Tech support	Tech-Support	Remote-1-web	Any Traffic	http	accept	Alert	Remote-1-gw	Any

Effectiveness of user-identity based rules could be further enhanced by implementing integration with corporate directory services and multi factor authentication.

- Many types of IPv4 traffic, such as that with invalid or private addresses, should be blocked by default.

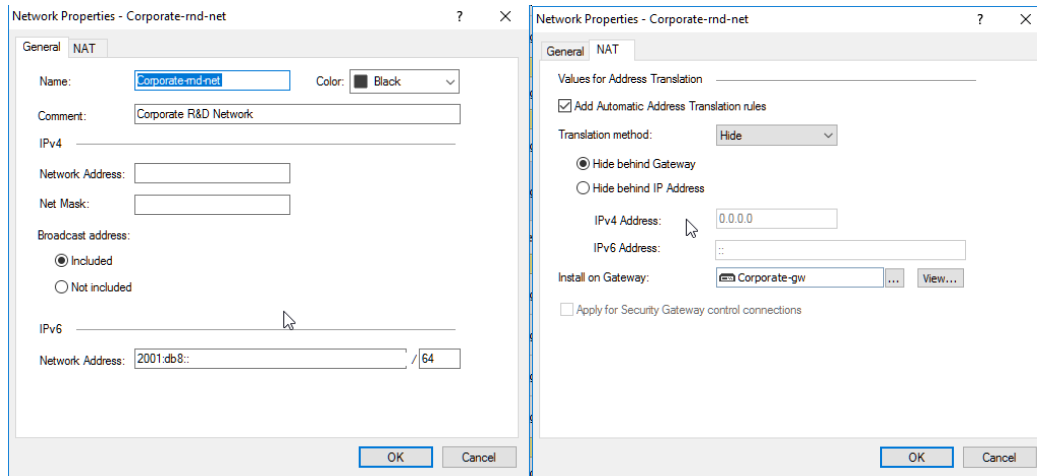
IP addresses defined as “Non-Unique” in the “Global Properties” are going to be treated as private:



In addition to these, other Martian IP addresses include 127/8 network and 224/3 multicast range. The term “Martians” generally refers to networks considered illegal to be routed on the Internet.

- Organizations should have policies for handling incoming and outgoing IPv6 traffic.

Check Point R77 can be configured to handle either IPv4 and/or IPv6. To properly handle IPv6, it should be enabled on the appliances, interfaces assigned IPv6 addresses and objects created with IPv6 properties and NAT defined, e.g.:



You may also implement IPv6 in IPv4 Intra Tunnel Inspection. R77 supports access control and IPS inspection of encapsulated IPv6 packets using the SIT\_with\_Intra\_Tunnel\_Inspection service. When using the SIT\_with\_Intra\_Tunnel\_Inspection service in a rule, the IPv6 packets are extracted and matched against all applicable rules in the Rule Base.

IPv4 Intra-Tunnel inspection (Rule 6)								
6	0	IPv6 Tunneling	Any	Any	Any Traffic	SIT_with_Intra_Tunnel_Inspection	accept	Log

Note: The location of the rule that contains the SIT\_with\_Intra\_Tunnel\_Inspection rule is not important. The extracted packets are matched against all rules in the Rule Base.



- *An organization should determine which applications may send traffic into or out of its network and make firewall policies to block traffic for other applications.*

Check Point firewalls can recognize the traffic by application and use Application and URL Filtering blade to permit or deny payload based on those criteria. As shown here:

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track
1	114K	Allow HR to browse MyHR.com site	HR	Internet	MyHR.com	Inform Inform Sensitive Information Once a day	Log
2	545K	Block sites which may cause liability	Any	Internet	Potential_Liability	Block Blocked Message	Log
3	0	Block High risk applications	Any	Internet	High Risk	Block High Risk Block	Log
4	1M	Block malwares	Any	Internet	Anonymizer	Block Blocked Message	Log
5	185K	Allow TeamViewer application for specific user - ticket #88721	John_Adams_Role	Any	TeamViewer	Allow	Log
6	623K	Allow remote admin for IT Dept only	IT_Department	Any	Radmin	Allow	Log
7	261K	Allow Facebook only to HR	HR	Internet	Facebook	Allow Download_1Gbps Down: 1 Gbps	Log
8	147K	Allow streaming only for Marketing, and verify access reason	Marketing	Internet	Vimeo YouTube	Ask Company Policy Once a day	Log
9	368K	Linkedin and Facebook are allowed for business purposes only	Any	Internet	Facebook LinkedIn	Inform Access Notification Once a day	Log
10	2M	Allow File sharing only for IT Department	IT_Department	Internet	P2P File Sharing	Allow	Log

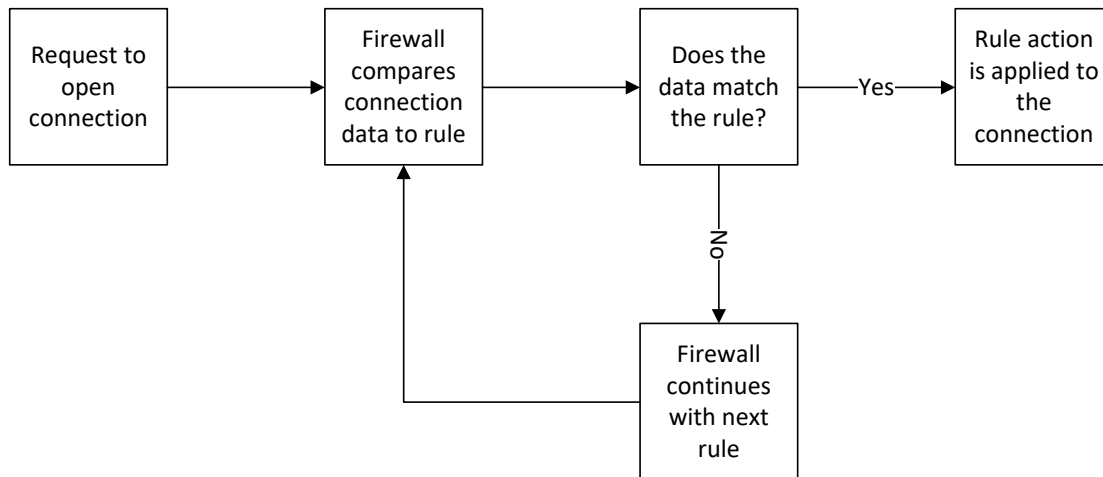
You may define additional custom applications and categories, as well as nest one inside the other to create policies suitable for your organization.

To improve your security stance even further, you can implement automated bidirectional communication with your users, informing them about company policy on use of the resources, requesting their consent to proceed or explaining why some of the applications are being blocked.

To better utilize available bandwidth and firewall's processing power you have means to limit the upload and download bandwidth for applications, on an individual rule basis.

## NIST 800-41 Revision 1 Section 5.2.2 Policy Configuration

Check Point firewalls inspect rules in a sequential manner from top to bottom of the policy and executes first rule matching traffic.



It is important to keep in mind the presence and relative placement of implied rules. As per Check Point:

1. First Implied Rule: You cannot edit or delete this rule and no explicit rules can be placed before it.
2. Explicit Rules: These are rules that you create.
3. Before Last Implied Rules: These implied rules are applied before the last explicit rule.
4. Last Explicit Rule: We recommend that you use the Cleanup rule as the last explicit rule.
5. Last Implied Rules: Implied rules that are configured as Last in Global Properties.
6. Implied Drop Rule: Drops all packets without logging. You cannot see, edit or delete this rule.

The following two explicit rules are considered necessary for a strong firewall security policy:

First Explicit Rule: Stealth rule that prevents direct access to the Security Gateway.

Last Explicit Rule: Cleanup rule that drops and logs all traffic that is not allowed by the earlier rules.

All other explicit rules are supposed to be placed between the two above-mentioned rules.

Since rules are processed sequentially, try to follow these principles:

First principle: More specific rules should supersede generalized rules.

Second principle: Rules that are likely to match more traffic should be placed closer to the top of the policies, while not contradicting the first principle.

The Hit Count feature, enabled by default, is there to assist you in making decisions regarding rule placement and utilization. If the "Hits" remain at "0", it is typically an indication of misconfigured rule, a case where conditions have not yet been met or, if the rule is applied to multiple gateways, a sign that some of them may have the Hit Count feature disabled.

For example, in this policy:

Policy

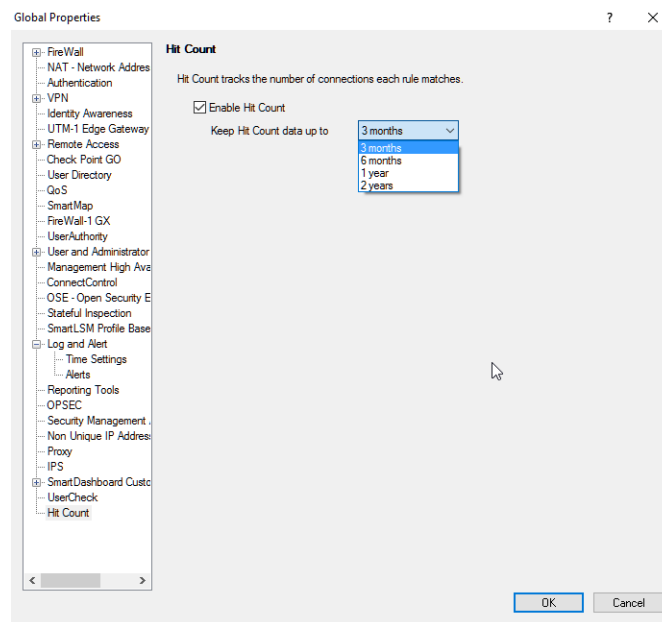
Search for IP, object, action, ...

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
Limit Access to Gateways Rule (Rule 1)										
1	214K	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any
VPN Access Rules (Rules 2-5)										
Rules for Specific Sites (Rules 6-8)										
6	7M	Outbound HTTP	Remote-2-internal	Any	Any Traffic	TCP http	Client Auth	Log	Remote-2-gw	Any
7	1K	Critical subnet	Corporate-internal-net	Corporate-fina Corporate-hr-n Corporate-rnd	Any Traffic	Any	accept	Log	Corporate-gw	Any
8	3M	Tech support	Tech-Support	Remote-1-web	Any Traffic	TCP http	accept	Alert	Remote-1-gw	Any
Identity Based Access (Rules 9-12)										
Common Rules - All Sites (Rules 13-19)										

Rule 7 Hit Count is “1K”, whereas rule 8 is “3M”. Unless there is a compelling reason to have those two rules in the order shown, it makes more sense to reverse the rule placement.

If you need to reset the Hit Count for a particular rule, follow instructions in [sk111832](#); if you must reset Hit Count for all the rules within the entire policy, follow [sk72860](#). You must be logged into the UserCenter to access these documents.

Hit Count could be configured to reflect percentage, value, level or any combination of these three parameters, as well as adjusted between 1 month and 2 years of historical data analysis. Duration is adjusted in Global Properties/Hit Count:



and further narrowed-down in the policy itself, by right-clicking on the rule number, selecting Hit Count/Timeframe and choosing the desired parameter.

Remember that the effectiveness of your security policy relies on a properly defined firewall topology and correct anti-spoofing settings. Do not relax anti-spoofing settings in the name of expedience!

The policy can be further enhanced by specifying time parameters for certain rules. For example, if you do not expect outbound connections to be established from subset of your environment outside of the work hours or on weekends, you may define the range of time those services should be available to your users. Time parameters could be specified in Firewall, Application and URL Filtering, DLP and QoS policies on an individual rule basis.

In cases where temporary access must be granted to certain resources and/or group of users, the **“Time”** parameters allow you to configure **“Activate on”** and **“Expire on”** parameters, preventing accidental retention of the rule past its intended application.

In the instances when anomalous attempts to access resources are observed, (for example indicative of APT), and actions should be taken immediately without going through formal policy review process and waiting for the policy application window, the **“Tools/Suspicious Activity Rules”** in the SmartView Monitor could be triggered for specified amount of time, to handle threat remediation until a more permanent solution could be created and applied in the rule set.

Another policy tool specific to IPS is **“Geo Protection”**. Rules limiting traffic from unlikely countries of origin could be implemented to minimize threat exposure. Exceptions to the Geo Protection rules could be configured to allow accessibility to a limited subset of resources that may have additional hardening implemented, whenever necessary.

When using a composite firewall policy (i.e. one policy with variable **“Apply To”** targets) it is important to take the topology of your network, as well as data flows, into consideration. For example, if you have two separate rules, each applied to two separate gateways, allowing same type of traffic, position those within the policy in such a way that the rule containing first gateway encountered by traffic will always be on top. You can group these rules in sections and create descriptive section headers explaining dependencies.

When creating section headers and rule descriptions, do not refer to any rules by their numbers. During policy lifetime your rules will change their position in the rule set. Similarly, do not refer to your policy rule numbers in your documentation; use description of the actual rule instead.

## NIST 800-41 Revision 1 Section 5.2.3 Logging and Alerts Configuration

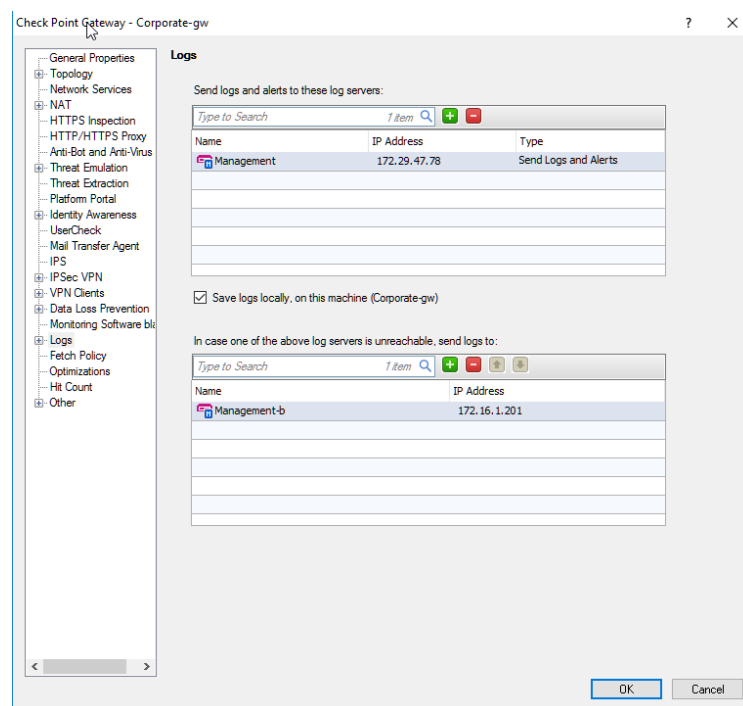
Check Point is renowned for its extensive and easy to read logging facilities. Its logging application could be effectively utilized for monitoring not only the traffic flowing through the Check Point appliances, but third party forwarded log events as well.

Each rule or action defined in the numerous Check Point blades could be configured to be logged.

Generally, it is a good practice to aggregate logs from multiple gateways, devices, appliances and clients to facilitate troubleshooting and forensic traffic analysis. Check Point “Logging and Status” blade could co-exist with other functions of the Management Servers or be enabled on dedicated physical or virtual appliances.

Although NIST 800-41 specifies that “whenever possible, the firewall should be configured both to store logs locally and to send them to a centralized log management infrastructure”, in most modern implementations logs are offloaded from execution modules. However, they could be logged locally as well, if required.

Multiple logging targets may be defined to allow for failover to secondary logging servers in the event where primary targets become unavailable. Additionally, you may elect to forward logs to a third party monitoring facility, such as SOC, using syslog. See [sk87560](#) for instructions.



It is important to properly size the processing power, memory, storage, and performance capacity for your logging servers. Depending on your business or regulatory requirements, logs may have to be rotated and preserved for a defined period before being destroyed.

Management functions audit logging is automatic and logs could be viewed in SmartView Tracker Management tab:

No.	Date	Time	Application	Subject	Operation	Object Type	Performed On	Changes
1	27Mar2009	10:33:35	SmartDashboard	User Certificate	Generate User Certific...	user	David	
2	27Mar2009	10:33:41	SmartDashboard	Object Manipulation	Create Object	user	David	
3	27Mar2009	10:33:55	SmartDashboard	Object Manipulation	Modify Object	user	David	Destination: added...
4	27Mar2009	10:35:10	SmartDashboard	Object Manipulation	Modify Object	firewall_policy	Standard	rule 1 - action: add...
5	27Mar2009	10:36:01	SmartDashboard	Policy Installation	Install Policy	firewall_application	California_GW	
6	27Mar2009	10:36:40	SmartDashboard	SIC Certificate	Initialize SIC Certificate	cpshared_applicati...	California.DMZ.Lag...	
7	27Mar2009	10:36:44	SmartDashboard	SIC Certificate	Revoke SIC Certificate	cpshared_applicati...	California.DMZ.Lag...	
8	27Mar2009	10:37:27	SmartDashboard	Policy Installation	Uninstall Policy	firewall_application	California_GW	
9	27Mar2009	10:38:21	SmartDashboard	Object Manipulation	Uninstall Policy	gateway_ckp	California.DMZ.Lag...	VPN was removed, ...
10	27Mar2009	10:38:21	SmartDashboard	Object Manipulation	Delete Object	firewall_application	firewall_applicatio...	
11	27Mar2009	10:38:21	SmartDashboard	Object Manipulation	Delete Object	vpn_application	vpn_application_C...	
12	27Mar2009	10:39:02	SmartDashboard	Revision Control	Create Version		Version 2	
13	27Mar2009	10:39:14	SmartDashboard	Revision Control	Revert to Version		Version 2	
14	27Mar2009	10:39:18	SmartDashboard	Administrator Login	Log Out			
15	27Mar2009	10:39:20	SmartDashboard	Administrator Login	Log In			
16	27Mar2009	10:39:29	SmartView Trac...	Administrator Login	Log Out			
17	27Mar2009	10:39:38	SmartView Trac...	Administrator Login	Log In			
18	27Mar2009	10:40:21	User Monitor	Administrator Login	Log In			

In addition to logging capabilities, every rule, as well as a change of state and management actions could be configured to generate alerts. Default alerting functions are defined in “Global Properties/Log and Alert/Alerts”:

**Global Properties Alerts**

**Alert Commands**

- Send popup alert to SmartView Monitor
- Run popup alert script
- Send mail alert to SmartView Monitor
- Run mail alert script: `internal_sendmail -s alert -t mailer root`
- Send SNMP trap alert to SmartView Monitor
- Run SNMP trap alert script: `internal_snmp_trap localhost`
- Send user defined alert no.1 to SmartView Monitor
- Run UserDefined script
- Send user defined alert no.2 to SmartView Monitor
- Run UserDefined 2 script
- Send user defined alert no.3 to SmartView Monitor
- Run UserDefined 3 script

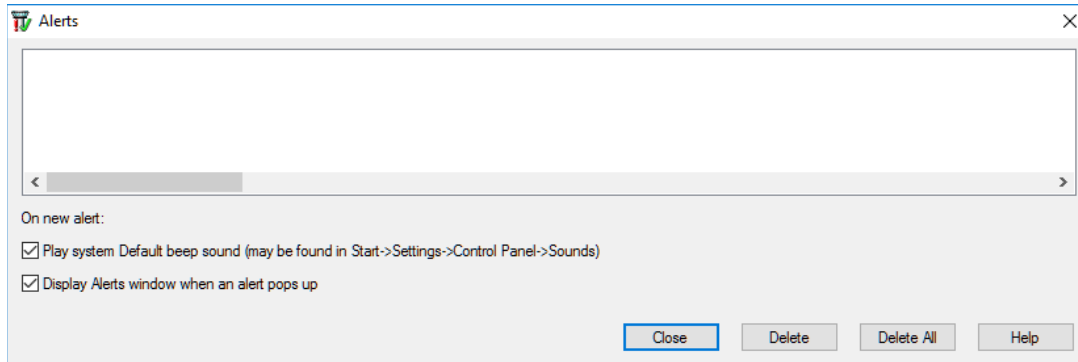
**System Alerts**

Set the default track option for this type of alert: **Alert**

- Alert
- Mail
- SNMP Trap
- User Defined Alert no. 1
- User Defined Alert no. 2
- User Defined Alert no. 3

OK Cancel

and include the ability to send popup alerts to SmartView Monitor “Alerts”, a proprietary Check Point notification client that could be started from “SmartView Monitor/Tools/Alerts”:



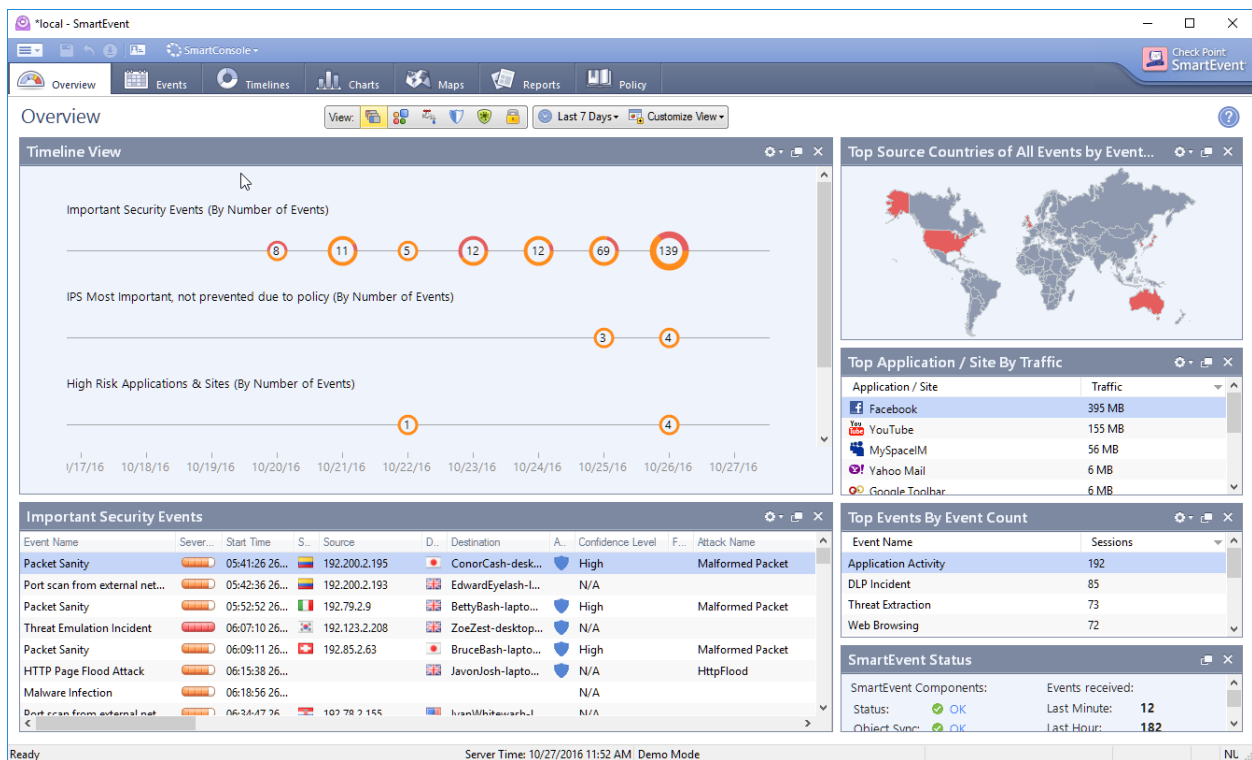
It is also possible to generate SNMP traps, email notification or run user defined scripts.

An advanced feature called SmartEvent is another tool that bridges logging, alerting and management capabilities.

Smart Event is comprised of two segments: Smart Event Server and Smart Event Correlation Unit. These could coexist on the same management server that contains other management blades or be hosted separately, depending on the overall volume of events your organization generates.

Smart Event Correlation Unit is responsible for aggregation and correlation of events from various components of your infrastructure. It is not limited to Check Point products.

The Smart Event Server and its corresponding SmartEvent management application present a dashboard view of aggregate information, allowing the administrators to make security assessments “at a glance”:



In addition to being an invaluable resource for visual representation of timelines, charts and comprehensive reporting capabilities, it is an incredibly powerful automation tool that could be configured to react to threats automatically by blocking source or activity for a defined time, as well as for triggering alerts and notifications.

Ability to create either Global Exceptions or exceptions on per-policy basis assures that production critical traffic is not affected.



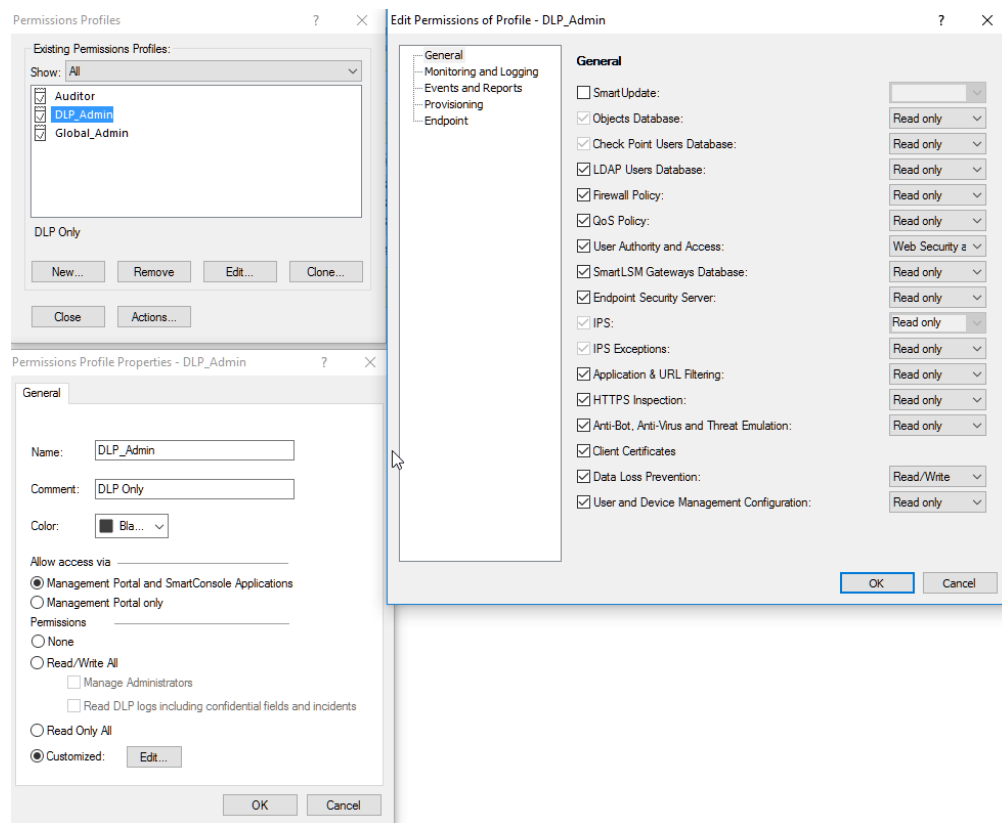
## NIST 800-41 Revision 1 Section 5.5 Management

Managing firewalls is an ongoing endeavor that should follow established documented policies. Responsibilities for certain aspects of management should be assigned and the execution of associated functions monitored.

Mostly associated with alterations of security policy and monitoring, things such as patching of vulnerabilities\*, installation of updates, backup and restore operations, all fall under this category.

Check Point Security Management server, when used in a single tenant environment, allows a single administrator to maintain the lock on the database for the Read/Write purposes at a time. All other administrators attempting to log on at the same time are prompted with notification regarding the person presently maintaining the lock and asked to log on in the Read-Only mode or to override the lock established by the currently logged-on administrator.

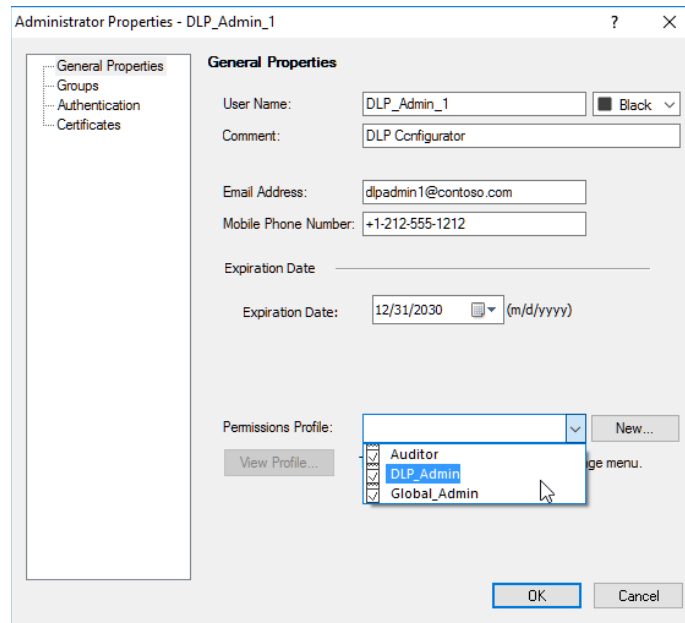
It is prudent to establish a clear hierarchy and separation of duties for the administrators. This could be accomplished using the SmartDashboard/Manage/Permission Profiles with great granularity:



Permissions assigned to each administrator should be formally documented and approved by management. Any alterations to administrative permissions should undergo a formal approval process and, likewise, should be documented.

\*For additional information about patch management, see [NIST SP 800-40 Version 2, Creating a Patch and Vulnerability Management Program](#).

Each administrator or group should have a permission profile with least privileges necessary to perform their jobs:



If your infrastructure relies on the RADIUS authentication, follow [sk72940](#) to integrate your Check Point Gaia appliances with it.

Please note that a single local administrative account created via “cpconfig” or during installation of Check Point products will always authenticate locally to prevent lockouts. Therefore, the complexity and length of the password assigned to it should, correspondingly, be substantial.

Check Point has a management module called “Workflow” that could be configured for either tracking of changes to the objects and policy, or a fully functional method for approval of changes in addition to tracking.

It may also be beneficial to implement a third-party solution for these purposes that, once configured, will remain outside of the purview of Check Point administrators. One such solution is a [Firemon](#) and it provides the following functionality:

- |                            |                               |                             |
|----------------------------|-------------------------------|-----------------------------|
| Plan configuration changes | Change control tracking       | Hidden rules report         |
| Clean-up policies          | Change control report         | Rule usage analysis         |
| Stay in compliance         | Immediate change notification | Object usage analysis       |
| Firewall-specific requests | Daily activity report         | Traffic flow analysis       |
| Rule recommendation        | Firewall complexity report    | PCI assessment              |
| Audit log                  |                               | Custom compliance reporting |

Having this or a similar tool at your disposal will greatly simplify your ability to adhere to the multiple compliance framework requirements.

## Conclusion:

Check Point Software Technologies provides its customers with a wide range of tools necessary to safeguard their businesses.

The growing complexity of modern IT infrastructures with an increased emphasis on security and compliance makes the roles of security architects and administrators more challenging than ever before.

Taking advantage of Check Point's products, with their unified architecture and highly integrated management tools, allows for implementation of an efficient in-depth security coverage for your essential technology resources. Utilizing these tools to their full capacity will substantially lighten your burden of achieving and maintaining compliance goals.