FIREMON

FireMon Security Manager

防火牆策略管理解決方案

目前隨著資訊化的加速，企業面臨的網路安全威脅也越來越大。因此企業往往購買了許多的網路安全設備部署在網路環境中，其中應用和部署最廣泛的網路安全設備之一就是防火牆。

防火牆是通過安全策略來進行安全防護，防火牆安全策略的配置對防火牆的安全防護作用起了不可或缺的作用。試想一台再好的防火牆設備，如果不配置安全策略，或者安全策略的配置錯誤，那麼這台防火牆就完全無法達到應有的安全防護作用，並且還會帶來許多安全隱患和安全事件。根據Gartner的統計，95%的防火牆安全事件均是由防火牆的配置錯誤而引起的。而另一份Gartner的報告表明，造成系統故障的原因有超過80%是由於人員失誤，包括配置失誤、流程失誤等。

因此，防火牆安全策略配置的正確性對於防火牆設備的安全防護作用非常重要。

但是許多企業目前對防火牆安全策略的管理缺乏有效的方法，使得防火牆安全策略處於「不透明」的狀態。最基本的兩個困惑之處有：

1）如何確定防火牆上的安全策略配置是正確的？

2）當收到業務部門提出安全策略配置需求申請時，該如何配置一條正確的策略？

一些典型的管理員關於安全策略的問題包括：

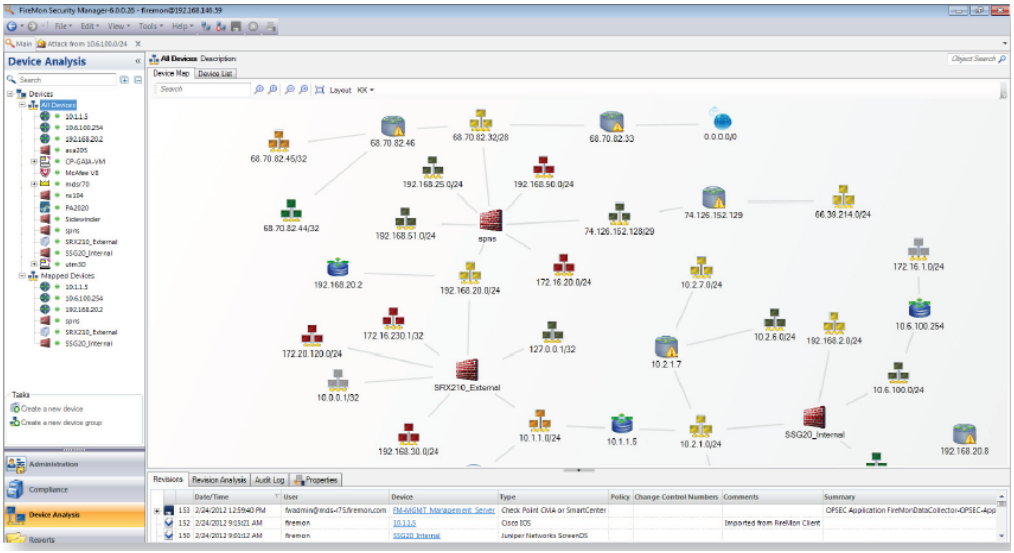
- 那些安全策略是多餘的？ 那些策略是無用的？
- 那個或那些安全策略被使用的最多、最頻繁？
- 這條安全策略的目的？誰設定的？什麼時間設定的？正在作用中嗎？
- 是否存在過於「寬鬆」的安全策略，允許了過多的流量通過？ 該如何收斂該條策略？
- 是否存在安全策略，允許了高危險端口流量的通過？
- 網路中某兩點間某服務是否可達？可到達的路徑是什麼？穿過了那些防火牆設備？ 命中了那些策略？
- 當收到業務部門提出的安全策略配置申請時，該如何配置策略？是否需要新增策略？該配一條什麼樣的策略？該在那一台防火牆上增加策略？這條新增的策略合規嗎？
- 防火牆的配置是否符合安全規範，如PCI、ISO27002等？
- 企業內部安全區域之間的存取規則，在防火牆上的安全策略是否符合這些存取規則呢？

因此，在防火牆的安全策略配置、變更時，包括新增策略、變更策略，或者刪除策略時，管理員操作依據較為模糊，缺少相關的數據報告或是科學分析，所以有時會出現防火牆安全策略配置上的缺陷或者錯誤，有些配置錯誤造成了客戶系統的故障。

現在有了 FireMon 的 Security Manager，這些頭痛的問題都將能迎刃而解！！

據 Gartner 統計，約 95%的防火牆安全事件是由於防火牆配置錯誤引起 !!

防火牆安全管理 Security Manager



Security Manager 可以協助管理員優化整合防火牆安全策略，瞭解當前防火牆策略的使用狀況，顯著改善防火牆運行效率及性能，並提升防火牆的安全性

FireMon Security Manager 可以協助管理員優化防火牆的安全策略，瞭解當前防火牆策略的使用狀況，可以查看那些策略是長期以來沒有被使用過，那些安全策略的使用率最高，可以查看某條安全策略實際的流量狀況，分析流量是如何穿過這條策略的；根據這些訊息，管理員就可以對安全策略進行優化，如清理掉一些不必要的策略，並且能夠準確瞭解到當前策略的使用效果等。良好的全圖形化介面將提升管理員對安全策略的可視性，這將大大提高管理員針對防火牆的安全管理效率。防火牆的管理將變得簡單、容易。

FireMon Security Manager 的典型功能包括：

安全策略變更管理

即時配置變更通知

FireMon Security Manager會即時監控防火牆，當防火牆的配置或者安全策略被變更時，指定的管理員會即時收到Security Manager發來的通知，告知管理員配置的變更以及變更狀況。

防火牆安全策略配置助手

當需要增加或修改防火牆安全策略時，可通過Security Manager的Policy Planner模組協助規劃安全策略的配置。Policy Planner能夠根據輸入的訊息，智能的分析是該如何配置策略，包括是否需要新的安全策略，如何需要，則會建議出所需配置的安全策略，包括配置的具體位置、配置的防火牆等。

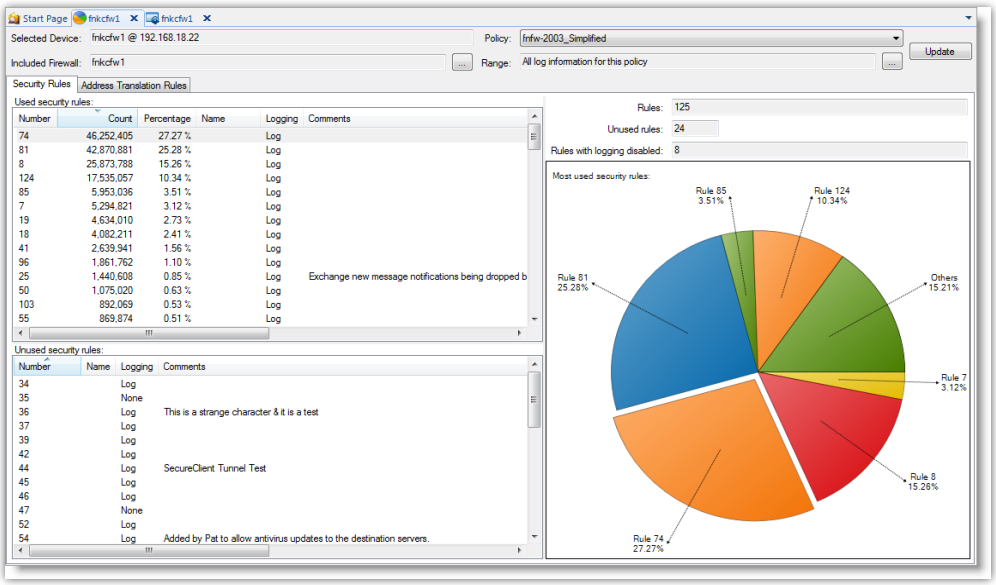
追蹤變更控制、不同時間點、不同品牌配置比對

記錄每次防火牆配置的修改，包括修改的詳細技術訊息。並且可比較不同時間點配置的差異，並詳細標記差異之處，使得管理員清楚地瞭解配置的變化，以及變化的過程。同時可比對不同品牌防火牆安全策略的差異。

統一格式導出所有防火牆的安全策略配置

能夠以統一的格式導出所管理防火牆上的所有安全策略配置，方便文件檔管理。

安全策略使用狀況分析

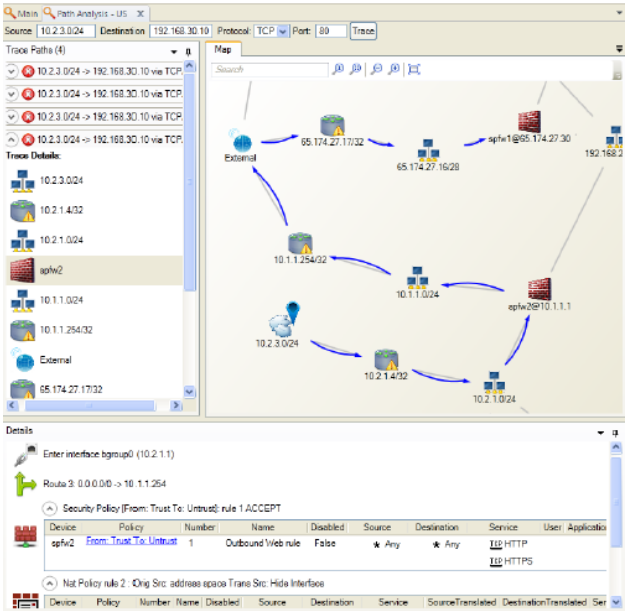


FireMon Security Manager記錄每條安全策略的被使用情況，並且通過圖餅圖方式顯示策略利用率報告。通過這個報告，你可以查看某台防火牆上安全策略的利用率狀況，或者那些策略是長期以來沒有被使用過。管理員通過該報告可以調整防火牆安全策略的順序，或者刪除長期命中率為零的安全策略。

對象(object)使用狀況分析

FireMon Security Manager 不僅能夠記錄每條安全策略的使用率狀況，還能夠記錄每天策略內的各個對象（object）的使用狀況，是否存在多餘的、無用的對象，管理員可以通過此訊息精簡策略配置，提升防火牆效率。

存取路徑分析（Access Path Analysis）



管理員可以利用 Security Manager 的 APA 功能，分析當前網路環境下，以及防火牆策略

配置下，系統內的兩個節點間的某服務是否可到達，並給出詳細報告，包括路徑、通過的設備、通過的防火牆設備命中的那一條策略等等。這樣管理員能夠方便的瞭解所配置的某條策略是否生效，或者是否需要增加新的安全策略來阻止系統內兩點間的某項服務。

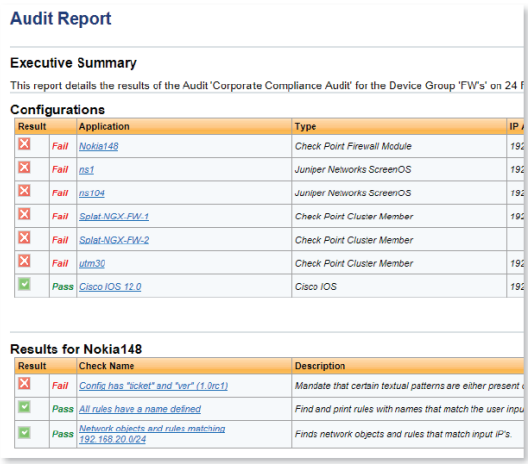
多餘安全策略分析

隨著網路複雜度的提升，防火牆的策略也變得日益龐大，而其中通常有大量的無用，或者多餘的安全策略。過多的安全策略嚴重降低防火牆的性能及效率。通過Security Manager，管理員可查看那些安全策略是不必要的多餘配置。可以根據該報告清理多餘的安全策略。

安全策略收斂及安全策略流量分析（Traffic Flow Analysis）

許多防火牆上均會存在一些過於「寬鬆」的安全策略，包括允許了過多的IP地址、允許了過多的服務端口，或者直接是“any”類型的安全策略。這不符合安全策略配置的一般性原則，需要進行「收斂」。這需要瞭解這些安全策略下的流量狀況，包括特定應用流量的佔比，如HTTP流量百分比多少，TCP端口443的佔比多少...等。通過Security Manager的Traffic Flow Analysis功能，管理員可查看任何一條安全策略的流量詳細訊息，包括各種應用的使用比率等。管理員可以根據該報告制定更加有針對性、更加準確的安全策略，進而提升防火牆的安全性。

防火牆配置合規性


Audit Report

Executive Summary

This report details the results of the Audit 'Corporate Compliance Audit' for the Device Group 'FW's' on 24 F

Configurations

Result	Application	Type	IP
Fail	Nokia148	Check Point Firewall Module	192
Fail	ns1	Juniper Networks ScreenOS	192
Fail	ns104	Juniper Networks ScreenOS	192
Fail	Splat-NGX-FW-1	Check Point Cluster Member	192
Fail	Splat-NGX-FW-2	Check Point Cluster Member	
Fail	utm30	Check Point Cluster Member	192
Pass	Cisco IOS 12.0	Cisco IOS	192

Results for Nokia148

Result	Check Name	Description
Fail	Config has "ticket" and "ver" (1.0rc1)	Mandate that certain textual patterns are either present
Pass	All rules have a name defined	Find and print rules with names that match the user inpu
Pass	Network objects and rules matching 192.168.20.0/24	Finds network objects and rules that match input IP's.

基於國際標準的合規性審查

Security Manager可根據國際規範，包括PCI或者ISO 27002等，審視防火牆的配置。審計報告中會顯示那些配置是不符合規範，並且會給出修改配置的建議。

安全區域存取規則合規性審查

在部署了防火牆的客戶，通常均劃分了一些安全區域。安全區域之間存取是受限制，制訂有相關的安全區域存取規則，並且這些存取規則是通過防火牆上的安全策略實現。如何確定防火牆上的策略是符合安全區域之間存取規則，通常只能透過管理員憑經驗檢查，費時、費力、且不一定準確。

利用Firemon Security Manager，管理員可將安全區域存取規則定義在系統中，並跟據此相關的防火牆進行合規性審查。這樣管理員可快速、準確的確定防火牆上策略配置是否符合安全區域存取規則。這樣操作可定期自動進行，結果也可輸出至第三方系統。

自行定義企業自身安全規範並進行安全合規性審查

許多客戶都有企業自身的安全政策。主要包括自定義危險端口、及安全區域存取規則等。

管理員可將企業的安全政策在 Security Manager 中進行定義，並且可據此對系統內防火牆設備

的安全策略配置進行合規性檢查，發現不合規的安全策略。可以自行定義非常複雜條件的安全規範，包括各種複雜查詢條件的組合(AND、OR、NOT...等)。查詢結果可按照管理員的指定格式進行輸出，如 CSV、XML、PDF、JSON 等。也可輸出到企業自身的管理系統。這些合規性審查報告，除了可即時查看外，也可定期自動發送給指定管理員。

部署

FireMon Security Manager 可部署在網路環境中任何 IP 可達位置。硬體方面，企業可以選擇 FireMon 的專用硬體產品，也可以選擇將 Security Manager 軟體安裝在系統伺服器上。並不需要在防火牆或者其他網路設備上安裝軟體，對企業網路安全方面的配置不會有任何改變。

可管理的防火牆設備

廠商	產品系列
CheckPoint	NG+系列各款防火牆，SmartCenter Provider-1。包括 CheckPoint 公司硬體平台，以及 Nokia IPSO 硬體平台
Cisco	PIX 系列，ASA 系列，FWSM 模組，各款 IOS 路由器，交換器
Dell	SonicWall 系列防火牆
F5	GTM，LTM、AFM
Fortinet	Fortigate 系列防火牆
Juniper	ScreenOS 系列，Junos 系列
McAfee	McAfee Firewall Enterprise 系列防火牆
Palo Alto Networks	PA 系列防火牆
Huawei	Eudemon 系列防火牆
HillStone	SG 系列防火牆
TopSec	NGFW4000 系列防火牆
DPtech	FW1000 系列防火牆
H3C	SecPath 系列防火牆

關於FireMon

FireMon是全球領先的防火牆安全策略管理及網路風險分析解決方案供應商，總部位於美國堪薩斯城。FireMon於2001年全球首家推出防火牆安全策略管理系統，帶領了該市場的興起。其中Security Manager產品能夠協助客戶管理防火牆上配置、發現防火牆配置中的問題、分析當前策略使用狀況、安全區域存取合規性審計、自定義安全規範審計等。而在防火牆策略變更時，Firemon的策略流程規劃模組(Policy Planner)可大大幫助客戶簡化流程，提高變更的準確性。另外Risk Analyzer是市場領先的網路漏洞分析系統，能夠協助管理員更加準確的瞭解當前網路安全的態勢。FireMon的產品被廣泛應用於金融機構、運營商、政府、中大型企業等。更多訊息，請存取 www.firemon.com。