

Skybox® Firewall Assurance

PCI Compliance, Change Assurance, Ruleset Optimization

Firewall Assurance позволяет менеджерам безопасности быстро оценить статус соответствия брандмауэра во время ручной проверки, снизить расходы на поддержание брандмауэра и соответствие требованиям. Пользователи могут визуализировать и определить потенциальные риски, которые требуют немедленного внимания, включая противоречивые правила брандмауэра и неверную конфигурацию, а также отслеживать историю изменений правил доступа и объектов.

С Firewall Assurance IT-отделы могут также проверить планируемые изменения сети, чтобы избежать человеческих ошибок и неверной конфигурации, что может привести к нарушению безопасности или соблюдения требований.

Прозрачность

Firewall Assurance собирает информацию с различных брандмауэров, нормализует данные и анализирует соответствие с передовыми практиками или индивидуальными политиками. Создается наглядная карта топологии брандмауэра. Ненужные, теньевые и устаревшие правила могут быть быстро найдены и исправлены с целью оптимизации и упрощения множества правил брандмауэра.

Аудиторские проверки по требованию

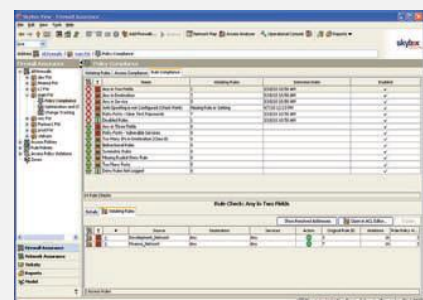
Аудиторские отчеты и показатели соответствия требованиям постоянно доступны и могут быть предоставлены аудиторам и руководству с целью документирования статуса соответствия. Это позволяет отслеживать соответствие брандмауэра с политиками безопасности и правилами. Отчеты Firewall Assurance предназначены для поддержки PCI DSS v1.2 и других нормативных требований.

Firewall Assurance

Firewall Assurance помогает организациям предварительно проверить изменения в брандмауэре, выявить проблемы доступа и другие потенциальных проблемы, прежде чем они повлияют на сеть. Кроме того, возможность отслеживать изменения позволяет сохранить, защищать, обслуживать и поддерживать историю модифицирования правил брандмауэра. Дополнительные возможности обеспечиваются через модуль Change Manager, либо с помощью API Skybox для настройки и интеграции с инструментами изменений третьей стороны. Приложения Web-сервиса предоставляют доступ интеграцию анализа политики с внешними приложениями управления процессом. Используя эти возможности, система может избежать простоев и потенциальных проблем доступа, которые, как правило, возникают из-за человеческих или конфигурационных ошибок.

" Это самый лучший инструмент для получения всей информации о рисках в одном месте. Skybox собирает воедино комплексную конфигурацию и уязвимость данных, чтобы показать нам уровни рисков, о которых мы и не задумывались".

**Руководитель программы
USAID, команда ISSO**



Преимущества Firewall Assurance

- Легко проследить историю изменений правил и объектов
- Поддержание и демонстрация соответствия брандмауэра нормативным требованиям
- Быстрый поиск и устранения потенциальных проблем безопасности
- Оптимизация множества правил брандмауэра и снижения ошибок в конфигурации
- Значительно уменьшить время, необходимое для управления брандмауэром



Firewall Assurance: datasheet

Ключевые черты

- Широкая поддержка всех вендоров брандмауэров, включая Check Point, Cisco, Fortinet, Juniper, McAfee, Symantec и др.
- Лучшие встроенные политики, основанные на стандартах PCI DSS и NIST
- Отслеживание истории изменений правил доступа и объектов
- Параллельное сравнение прошлых, текущих и будущих конфигураций брандмауэра
- Анализ путей доступа брандмауэра
- Анализ использования и оптимизация правил
- Настраиваемые политики доступа: обнаружение нарушений, анализа корневых причин и управление
- Автоматизированный анализ соответствия доступа
- Анализ *What-if* для виртуальной проверки запланированных изменений брандмауэра
- Правило соответствия - запустить проверку правил и просмотреть на уровне брандмауэра или политик
- Аудиторские отчеты и метрики соответствия
- Дополнительный модуль Change Manager добавляет полноценные возможности контроля над процессом изменений брандмауэра

Характеристики

Поддерживаемые ОС:

Windows 7, Windows Server 2008, Windows Server 2003 (32/64 bit) XP Professional SP2 или выше, Vista Red Hat Enterprise Linux v.4 (32/64 bit), v.5 (64 bit) CentOS

Минимальные системные требования*

- Память: 4ГБ RAM
- CPU: 2.8 GHz
- Хранилище: 20GB

Поддерживаемые устройства – Сетевые устройства

Check Point VPN-1, Firewall-1 and Provider-1, Fortinet Fortigate 2.x, 3.x, Nokia Appliances под управлением Check Point FW-1/VPN-1, McAfee Firewall Enterprise (Sidewinder) G2, V.6, маршрутизаторы Cisco под управлением Cisco IOS 11.x, 12.x; Cisco PIX, ASA, FWSM, Juniper Netscreen, SSG, ISG под управлением ScreenOS 4.x, 5.x, 6.x, Network and Security Manager (NSM), Symantec SGS

Поддерживаемые устройства – Система управления

Cisco Works

* Узнайте дополнительную информацию, исходя из ваших конкретных потребностей.



www.skyboxsecurity.com

Headquarters: Skybox Security, Inc. - 2099 Gateway Place, Suite 450 - San Jose, California 95110 USA
Phone: +1 (866) 441 8060 - Phone: +1 408 441 8060 - Fax: +1 408 441 8068

Copyright © 2011 Skybox Security, Inc. All rights reserved. Skybox and CertiFire are trademarks of Skybox Security, Inc. All other registered or unregistered trademarks are the sole property of their respective owners.