

CHECK POINT NG

РУКОВОДСТВО ПО АДМИНИСТРИРОВАНИЮ

В книге представлены все необходимые инструкции по использованию комплекса продуктов Check Point Next Generation, а также инструменты для создания корпоративной системы информационной безопасности. Check Point VPN-1/FireWall-1 уже многие годы находится далеко впереди конкурентов, а версия Next Generation устанавливает новые стандарты в технологиях защиты информации. Авторы не рассчитывали на какой-то опыт предыдущей работы с продуктами Check Point, поэтому в книге последовательно представлены методы установки и настройки VPN-1/FireWall-1 Next Generation, управление сетевыми объектами, создание и внедрение политики безопасности. Подробно рассмотрены схемы аутентификации S/Key, SecureID, OS Password, RADIUS и др., описаны форматы представления информации и отчетности, возможности Check Point по защите удаленных VPN-клиентов с помощью ПО Secure Client и другие аспекты использования продуктов линейки NG.



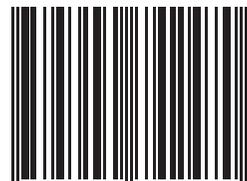
www.dmk-press.ru

Internet-магазин
www.aliants-kniga.ru

Книга-почтой:
Россия, 123242, Москва, а/я 20
e-mail: orders@aliants-kniga.ru

Оптовая продажа:
"Альянс-книга"
(495)258-9194, 258-9195
e-mail: books@aliants-kniga.ru

ISBN 5-94074-247-5



9 785940 742470 >



СНЕСК РОІНТ NG

РУКОВОДСТВО ПО
АДМИНИСТРИРОВАНИЮ

CHECK POINT NG

РУКОВОДСТВО ПО АДМИНИСТРИРОВАНИЮ

Дрю Симонис
Кори С. Пинкок
Даниель Клигерман

Дуг Максвелл
Джеф Винс
Симон Десмеулес

Перевод с английского
Базаренко Н. В., Мякишева А. А.



Check Point

NG

Серия «Информационная безопасность»

Руководство по администрированию

Перевод с английского
Базаренко Н. В., Мякишева А. А.
Под общей редакцией
Мякишева А. А.

Дрю Симонис
Кори С. Пинкок
Даниель Клигерман
Дуг Максвелл
Джеф Винс
Симон Десмеулес



УДК 004.056
ББК 32.973.202
С37

С37 **Симонис Д. и др.**

Check Point NG. Руководство по администрированию: Пер. с англ. – М.: Компания АйТи: ДМК Пресс: ТЕТРУ. – 544 с.: ил. (Серия «Информационная безопасность»).

ISBN 5-94074-247-5 (ДМК Пресс) – 5-98396-002-4 (ТЕТРУ)

В книге представлены все необходимые инструкции по использованию комплекса продуктов Check Point Next Generation, а также инструменты для создания корпоративной системы информационной безопасности. Check Point VPN-1/FireWall-1 уже многие годы находится далеко впереди конкурентов, а версия Next Generation устанавливает новые стандарты в технологиях защиты информации. Авторы не рассчитывали на какой-то опыт предыдущей работы с продуктами Check Point, поэтому в книге последовательно представлены методы установки и настройки VPN-1/FireWall-1 Next Generation, управление сетевыми объектами, создание и внедрение политики безопасности. Подробно рассмотрены схемы аутентификации S/Key, SecureID, OS Password, RADIUS и др., описаны форматы представления информации и отчетности, возможности Check Point по защите удаленных VPN-клиентов с помощью ПО Secure Client и другие аспекты использования продуктов линейки NG.

Original English language edition published by Syngress Publishing, Inc. Copyright © by Syngress Publishing, Inc. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельца авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно остается, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможный ущерб любого вида, связанный с применением содержащихся здесь сведений.

Все торговые знаки, упомянутые в настоящем издании, зарегистрированы. Случайное неправильное использование или пропуск торгового знака или названия его законного владельца не должно рассматриваться как нарушение прав собственности.

ISBN 1-928994-74-1 (англ.)

Copyright © by Syngress Publishing, Inc.

ISBN 5-94074-247-5 (ДМК Пресс)

© Перевод на русский язык. Компания АйТи

ISBN 5-98396-002-4 (ТЕТРУ)

© Оформление. ДМК Пресс

© Издание. ТЕТРУ

Содержание

Сервер управления и шлюзы межсетевых экранов работают под управлением следующих операционных систем:

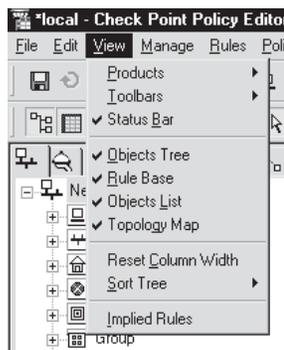
- Windows 2000 с или без Service Pack 1
- Windows NT 4.0 с Service Pack 4 или выше
- Sun Solaris 8
- Sun Solaris 7
- RedHat Linux 6.2, 7.0 и 7.2

Предисловие	19
Глава 1. Введение в Check Point Next Generation	23
Введение	24
Описание компонентов архитектуры Check Point SVN	25
VPN-1/FireWall-1	27
Account Management	30
SecuRemote/SecureClient	31
Reporting Module	33
Модуль Check Point High Availability	35
Модуль UserAuthority	37
Модуль FloodGate-1	38
Meta IP	39
VPN-1/FireWall-1 – компонент SVN	41
Модуль управления VPN-1/FireWall-1	42
Графический интерфейс пользователя	48
Policy Server	54
Технология Firewall	55
Проxy-сервер и пакетный фильтр	55
Инспекционный механизм FireWall-1	58
Резюме	62
Конспекты	64
Часто задаваемые вопросы	67
Глава 2. Установка и конфигурирование VPN-1/FireWall-1 Next Generation	69
Введение	70
Начало работы	70
Получение лицензий	72

6 Check Point NG. Руководство по администрированию

Настройка и внедрение...	Защита хоста	72
	Маршрутизация и сетевые интерфейсы	75
Установка лицензий	Конфигурирование DNS	78
Если ваши лицензии сохранены в файле с расширением .lic (например, license.lic), с помощью кнопки Fetch from File... можно вызвать обозреватель файловой системы. Когда вы найдете файл *.lic, нажмите кнопку Open , и лицензия будет импортирована в систему.	Подготовка к установке VPN-1/FireWall-1 NG	79
	Обновление версии	86
	Установка Check Point VPN-1/FireWall-1 NG на Windows	87
	Установка с CD	87
	Конфигурирование Check Point VPN-1/FireWall-1 NG на ОС Windows	99
	Деинсталляция Check Point VPN-1/FireWall-1 NG на ОС Windows	114
	Деинсталляция VPN-1 и FireWall-1	114
	Удаление компонента SVN Foundation	116
	Деинсталляция интерфейсов управления	119
	Установка Check Point VPN-1/FireWall-1 NG на ОС Solaris	119
	Установка с CD	120
	Конфигурирование Check Point VPN-1/FireWall-1 NG на Solaris	128
	Деинсталляция VPN-1 & FireWall-1	143
	Деинсталляция SVN Foundation	146
	Деинсталляция ПО клиентов управления	149
	Установка Check Point VPN-1/FireWall-1 NG на платформу Nokia	150
	Установка пакета программ VPN-1/FireWall-1 NG	151
	Конфигурирование VPN-1/FireWall-1 NG на платформе Nokia	155
	Резюме	158
	Конспекты	160
	Часто задаваемые вопросы	163
	Глава 3. Использование графического интерфейса	165
	Введение	166
	Управление объектами	166
	Объекты сети	168
	Сервисы	184

Меню View



Ресурсы	190
Приложения OPSEC	192
Серверы	192
Внутренние пользователи	196
Время	196
Виртуальные соединения	197
Добавление правил политики	198
Правила	199
Глобальные свойства	202
Скрытые правила в FireWall-1	202
Функция SYNDefender	204
Сервер безопасности	205
Аутентификация	205
VPN-1	205
Панель Desktop Security	206
Графический интерфейс пользователя	206
Высоконадежный шлюз	206
Высоконадежное управление	206
Stateful Inspection	206
LDAP Account Management	207
Адресная трансляция	207
ConnectControl	207
Open Security Extension	207
Log and Alert	207
SecureUpdate	207
Log Viewer	210
Выбор столбцов	212
Статус системы	213
Резюме	215
Конспекты	216
Часто задаваемые вопросы	218
Глава 4. Создание политики безопасности	219
Введение	220
Основа для создания политики безопасности	220

8 Check Point NG. Руководство по администрированию

Отказоустойчивость системы управления

При проведении синхронизации вручную есть два режима работы:

■ **Synchronize Configuration files only.**

Если выбран этот режим, на станциях управления будут синхронизированы только базы пользователей и конфигурационные файлы.

■ **Synchronize Fetch, Install and Configuration files.**

В этом режиме также синхронизируются скомпилированные файлы политик, что позволяет модулям МСЭ осуществлять взаимодействие с резервной станцией управления.

Ответы на часто задаваемые вопросы

Каким образом следует осуществлять конфигурирование правил NAT вручную? Или лучше использовать FireWall-1 для создания их автоматически?

Это не важно, каким образом будут созданы правила NAT, поскольку результат будет один и тот же. При автоматическом генерировании правил NAT необходимо постоянно проверять базу правил NAT, чтобы быть уверенными в том, что она выглядит и будет работать так, как мы ожидаем. Таким образом, ответ на этот вопрос в большей степени зависит от того, с чем более комфортно работать – с NAT или FireWall-1.

Как написать политику безопасности	221
Проектирование решения	225
Архитектура Firewall	225
Написание политики	226
Внедрение политики безопасности	230
Политика первоначальная и по умолчанию	230
Транслирование политики безопасности компании в правила редактора политик	232
Работа с правилами	244
Опции политики	247
Установка политики безопасности	250
Файлы политики безопасности	251
Резюме	253
Конспекты	253
Часто задаваемые вопросы	255

Глава 5. Применение адресной трансляции **257**

Введение	258
Соккрытие сетевых объектов	258
Маршрутизация и ARP	263
Конфигурирование статической адресной трансляции	265
Статический источник	265
Статический адрес получателя	269
Маршрутизация и ARP	271
Правила автоматической NAT	272
Автоматическое конфигурирование сокрытия	272
Автоматические правила для статической трансляции	274
Маршрутизация и ARP	276
Глобальные свойства NAT	277
Резюме	280
Конспекты	281
Часто задаваемые вопросы	282

Управление доступом пользователей

Для настройки пользовательской аутентификации создайте новое правило в политике безопасности, в поле **Source** щелкните правой кнопкой мыши и выберите пункт **Add User Access**.



Глава 6. Аутентификация пользователей 285

Введение	286
Схемы аутентификации FireWall-1	286
S/Key	287
SecureID	288
Пароль операционной системы	288
Внутренние пароли	289
RADIUS	290
AXENT Pathways Defender	291
TACACS	292
Описание пользователей	293
Создание пользователя «по умолчанию»	294
Создание и использование шаблонов	295
Создание групп пользователей	298
Пользовательская аутентификация	299
Клиентская аутентификация	305
Сравнение пользовательской и клиентской аутентификации	310
Сессионная аутентификация	311
Сессионная аутентификация в сравнении с клиентской и пользовательской	317
Аутентификация на серверах LDAP	318
Создание объекта сервера LDAP	319
Администрирование LDAP	322
Резюме	328
Конспекты	329
Часто задаваемые вопросы	331

Глава 7. Открытая безопасность и фильтрация по содержанию 333

Введение	334
Приложения OPSEC	334
Протокол перенаправления содержимого	336
Создание объектов	336
Создание CVP-ресурса	337

10 Check Point NG. Руководство по администрированию

Приложения OPSEC

- Существует три типа серверных приложений OPSEC: CVP, UFP и AMON.
- Клиентские приложения OPSEC, как правило, служат для отправки или получения данных из VPN-1/FireWall-1, они не участвуют в процессе контроля трафика, как серверы.
- ELA позволяет другим приложениям посылать свою отчетность в базу VPN-1/FireWall-1 для ее консолидации в единой точке.
- LEA используется для получения данных из центральной базы отчетности МСЭ за определенный период или в реальном времени.
- SAM позволяет системам обнаружения атак (IDS) изменять политику безопасности для блокировки вредоносного трафика.
- OMI служит для взаимодействия с базой объектов VPN-1/FireWall-1.

Создание правила с использованием ресурсов	340
CVP-группа	341
Протокол фильтрации URI	343
Создание объектов	343
Создание URI-ресурса с использованием UFP	345
Использование ресурсов в правилах политики безопасности	348
Группы UFP	349
Мониторинг приложений	350
Клиентские приложения OPSEC	350
Интерфейс отслеживания событий	351
Интерфейс экспорта отчетности	352
Мониторинг подозрительной активности	353
Интерфейс управления объектами	353
Интерфейс управления Check Point UserAuthority API	354
Дополнительные возможности ресурсов	354
URI-ресурсы	355
SMTP-ресурсы	361
FTP-ресурсы	365
TCP-ресурсы	367
Резюме	370
Конспекты	372
Часто задаваемые вопросы	375

Глава 8. Управление политиками и отчетностью 379

Введение	380
Оптимизация производительности в Check Point VPN-1/FireWall-1	381
Настройка производительности в NG	381
Администрирование NG для наивысшей производительности	384
Мониторинг NG для наивысшей производительности	389
Администрирование Check Point VPN-1/FireWall-1 NG для повышения эффективности работы	394