# FortiClient v5.0

#### Руководство по администрированию

9 января 2013

04-501-183401-20130109

Copyright © 2013 Fortinet, Inc Все права защищены. Fortinet ®, FortiGate ® и FortiGuard ®, являются зарегистрированными товарными знаками компании Fortinet, Inc, и другие имена Fortinet здесь, могут также являться товарными знаками из Fortinet. Все остальные названия продуктов и компаний могут являться товарными знаками соответствующих владельцев. Показатели производительности, содержащиеся здесь были достигнуты во внутренние лабораторные тесты в идеальных условиях и производительности могут отличаться. Сетевые переменные, различных сетевых средах и другие условия могут влиять результатах. Ничто в настоящем документе не представляет любой обязательством от Fortinet. Fortinet отказывается от всех гарантий, явных или подразумеваемых, за исключением степени Fortinet входит в обязательный письменный договор, подписанный главным юрисконсультом компании Fortinet, с покупателем, что прямо гарантирует, что выявленные продукты будет работать в соответствии с показатели эффективности в данном документе. Для полной ясности, любая такая гарантия будет ограничена производительности в том же идеальные условия, как в компании Fortinet внутренних лабораторных тестов. Fortinet отказывается полностью от всяких гарантий. Fortinet оставляет за собой право изменять, модифицировать, передавать или иным образом пересмотреть данный документ без уведомления, и самые последние версии издания должны быть применимо.

Техническая документация docs.fortinet.com База знаний kb.fortinet.com Обслуживания клиентов и поддержки support.fortinet.com Услуги по обучению training.fortinet.com FortiGuard fortiguard.com Документ Обратная связь techdocs@fortinet.com Изменения регистрации Дата Изменить описание 2012-11-02 Первый релиз. 2012-11-07 Обновлены скрипты глав. Этот документ в настоящее время включают как Windows, и Mac OS X. Это Важно отметить, что не все функции доступны для Windows, доступны для Mac OS X. 2012-11-15 Обновленный IPsec и SSL VPN-главе. 2012-11-22 Добавлено примечание о FortiClient Лицензия на FortiAuthenticator. 2012-11-27 Обновлен команды сценария, чтобы соответствовать изменениям в FortiClient v5.0 Ссылка XML.

#### 2013-01-09

Обновлено для FortiClient v5.0 релиза патча 1. Удалены XML главе см. в FortiClient v5.0 Справочник по XML для получения дополнительной информации. Удалены FortiClient главе средствах см. FortiClient

Примечания к выпуску для получения дополнительной информации.

# Введение

FortiClient была полностью заново разработанный для версии 5.0. FortiClient обеспечивает всесторонний решения сетевой безопасности для конечных точек, в то время как улучшение видимости и контроля. FortiClient позволяет управлять безопасностью нескольких конечных устройств FortiGate от интерфейса.

Этот документ содержит обзор FortiClient v5.0.

#### Лицензирование

Лицензирования на FortiGate на основе количества зарегистрированных клиентов. FortiGate 40С и выше модели поддерживают 10 (десяти) бесплатно управляемых FortiClient лицензий. Для получения дополнительной управляемых

клиентов, обновленная должна быть приобретена лицензия. Максимальное количество управляемых клиентов изменяется в зависимости от модели устройства.

# Клиент пределы

Этот документ был написан для FortiClient v5.0 Патч Release 1 для Windows. Не все функции описанное в этом документе поддерживаются для FortiClient v5.0 Патч Release 1 лля Mac OS X. Модель FortiGate Бесплатная регистрация FortiClient лицензии на обновление SKU FortiGate 40, 60, 80 серии, VM00 10 N/AFortiGate 100, 200, 300, 600, 800 серии, VM01/VM01-Xen, VM02/VM02-Xen 10 1000 регистраций клиентов FCC-C0103-LIC FortiGate 1000, 3000, 5000 серий, VM04/VM04-Xen, VM08/VM08-Xen 10 3000 регистраций клиентов FCC-C0105-LIC В высокой доступности (НА) конфигураций, всех членов кластера требует лицензионный ключ для обновления. Для получения дополнительной информации, зайдите в www.forticlient.com. Fortinet Технологии Инк FortiClient v5.0 Руководство администратора

## Поддерживаемые операционные системы

OC Windows Microsoft Windows 8 (32-разрядная и 64-разрядная версия) Microsoft Windows 7 (32-разрядная и 64-разрядная версия) Microsoft Windows Vista (32-разрядная и 64-разрядная версия) Microsoft Windows XP (32-разрядная версия) Mac OS X Mac OS X v10.8 Mountain Lion Mac OS X v10.7 Lion Mac OS X 10.6 Snow Leopard

# Минимальные системные требования

**OC** Windows Microsoft Internet Explorer 8.0 или более поздней OC Windows совместимый компьютер с процессором Pentium или эквивалентный Совместимой операционной системы и минимального ОЗУ: 512 МБ 600 Мб свободного места на жестком диске Родные Microsoft TCP / IP протокол связи Родные Microsoft программа дозвона для коммутируемого соединения Ethernet NIC для сетевых соединений Беспроводной адаптер для беспроводного подключения к сети Adobe Acrobat Reader или другой PDF Reader для инструкция MSI Installer 3.0 или более поздняя версия Mac OS X Процессор Intel 256 Мб оперативной памяти 20 МБ на жестком диске (HDD) пространства ТСР / IР протокол связи Ethernet NIC для сетевых соединений Беспроводной адаптер для беспроводного подключения к сети.

# Пожалуйста, ознакомьтесь с FortiClient v5.0 Патч Release 1 (Windows) или выпуске FortiClient

# Patch v5.0 Release 1 (Mac OS X) Заметки о выпуске перед

# обновлением. Текст документа доступен

на обслуживание клиентов и поддержка.

# Что нового в версии 5.0 FortiClient

Резюме усовершенствования

Ниже приведен список усовершенствований в FortiClient v5.0 (включая патч Выпуск 1): Защита от вирусов и вредоносных

Защиту от новейших вирусов и нежелательных программ (рекламных / опасное) угроз. Антивирусный клиент, является бесплатным и автоматическое обновление каждые три часа.

Application Firewall

Блок, позволит и контролировать приложения, отправлять трафик на сети.

Bring Your Own Device (BYOD)

Диагностический инструмент

Усовершенствования консоли FortiClient

Управление конечными точками использованием FortiGate, в том числе:

Автоматическая регистрация конечных точек и инициированные пользователем регистрации конечных точек.

Развертывание VPN (IPsec / SSL) конфигурации.

Включить / отключить антивирусную защиту в реальном времени.

Управление / развертывания веб-фильтрации и настройки Application Firewall.

Регистрация по IPsec VPN или SSL-VPN.

FortiGuard Analytics

Автоматически отправлять подозрительные файлы в сети FortiGuard для анализа.

Поддержка локализации

Родительский контроль / Web Filter

Блок, позволяют, предупреждают и мониторинга веб-трафика на основе категорий.

Помните, несколько FortiGates для регистрации Контроль рабочего места.

Удаленный доступ (IPsec и SSL VPN)

Безопасные виртуальные частные сети (VPN) доступ к вашей сети.

Поддержка нескольких шлюзов для одного туннеля.

Поиска и удаления руткитов

Single Sign-On агента мобильности с поддержкой FortiAuthenticator / FSSO Collector агент Поддержка автоматического выполнения пользовательского сценария партию через туннель IPsec VPN

Поддержка нескольких (максимум 10) Шлюз IP / FQDN в одном конфигурации IPsec VPN Поддержка XML-конфигурации

VPN из системного трея

Этот документ был написан для FortiClient v5.0 Патч Release 1 для Windows. Не все функции описанное в этом документе поддерживаются для FortiClient v5.0 Патч Release 1 для Mac OS X.

Fortinet Технологии Инк

VPN автоматического подключения / всегда

Поддержите возможность автоматического подключения к туннелю VPN без вмешательства пользователя.

Поддержите возможность настройки VPN, чтобы всегда быть подключены.

Поиск уязвимостей

Определение системы и приложений уязвимости.

# Установка FortiClient на компьютере OC Windows

# Следующие инструкции помогут вам хотя установка FortiClient на OC Windows компьютер.

Чтобы установить FortiClient

1. Дважды щелкните на исполняемый файл FortiClient для запуска мастера установки. Мастер установки

FortiClient установить на ваш компьютер.

Рисунок 1: Экран приветствия.



2. Прочитайте лицензионное соглашение и нажмите Далее, чтобы продолжить. У Вас есть возможность распечатать Лицензионное соглашение на этом экране. Рисунок 2: Лицензионное соглашение.

Fortinet Pr	oduct License	Agreement / E	ULA and Warranty T	erms 🔺
Trademark	s and Copyrig	ht Statement		
Fortinet <sup>®</sup> , For other Fortinet Fortinet. All or owners. Copy are subject to reproduced in translation, tr stipulated by	tiGate <sup>®</sup> , and Forti names herein ma ther product or co right © 2002-2013 change by Fortine any form or by an ansformation, or the United States	Guard® are register ay also be trademark mpany names may b I Fortinet, Inc., All Ri et without prior notic y means or used to r adaptation without Copyright Act of 197	ed trademarks of Fortinet, is, registered or otherwise e trademarks of their resp ghts reserved. Contents a e. No part of this publicat nake any derivative such a permission from Fortinet, 6.	Inc., and b, of nd terms tion may be as Inc., as
		ont		

3. Выберите Изменить, чтобы выбрать альтернативный папку назначения для установки. Выберите Далее, чтобы продолжиться. Рисунок 3: Выбор папки назначения

Destination Folder Click Next to install to the default folder or click Change to choose another	
Install FortiClient to:	
C:\Program Files (x86)\Fortinet\FortiClient\	
Change	
Back Next Cancel	

4. Выберите Установить, чтобы продолжить. Рисунок 4: Все готово для установки FortiClient.

Ready to install FortiClient	
Click Install to begin the installation. Click Back to review installation settings. Click Cancel to exit the wizard.	w or change any of your
Back	Install

5. Выберите Готово для выхода из мастера установки FortiClient. Рисунок 5: Установка завершена

Completed the FortiClient Setup Wizard	
Click the Finish button to exit the Setup Wizard.	
Back	Cancel

6. При новой установке FortiClient, вам не нужно, перезагруживать систему. При обновлении FortiClient версии, вы должны перезагрузить систему для изменения конфигурации FortiClient вступили в силу. Выберите Да, чтобы перезагрузить компьютер сейчас, или Нет, чтобы вручную перезагрузку позже. Рисунок 6: Перезапуск системы подтверждения.

i	You must restart your system for the configuration changes made to FortiClient to take effect. Click Yes to restart now or No if you plan to manually restart later.		
	Yes	No	

7. Для запуска FortiClient, дважды щелкните значок на рабочем столе ярлык. <u>Рисунок 7: Вы</u>берите FortiClient ярлык для запуска



# Установка FortiClient на компьютере Mac OS X

Следующие инструкции помогут Вам для установки FortiClient на Mac OS X компьютер.

Чтобы установить FortiClient

1. Дважды щелкните FortiClient, чтобы запустить установщик FortiClient.

FortiClient Installer установит FortiClient на вашем компьютере. Выберите Продолжить. Рисунок 8: Экран приветствия



2. Прочитайте лицензионное соглашение и выберите Продолжить. У вас есть возможность распечатать или сохранить соглашение на программное обеспечение на этом экране. Вам будет предложено согласиться с условиями действия лицензионного соглашения. Рисунок 9: Лицензионное соглашение.

000

Install FortiClient

Software License Agreement



8

Continue

Go Back

4. Выберите Установить, чтобы выполнить стандартную установку на этом компьютере. Вы можете изменить установки местоположение от этого экрана.

Рисунок 11: Экран типа установки.

00	🥥 Install FortiClient 🖉
	Standard Install on "Macintosh HD"
<ul> <li>Introduction</li> <li>License</li> <li>Destination Select</li> <li>Installation Type</li> <li>Installation</li> <li>Summary</li> </ul>	This will take 19.4 MB of space on your computer. Click Install to perform a standard installation of this software for all users of this computer. All users of this computer will be able to use this software.
	Change Install Location
	Go Back Install

5. В зависимости от вашей системы, вам может быть предложено ввести системный пароль.

Рисунок 12: Введите системный пароль, чтобы продолжить

•••	Install Forti Client	
⊜ Intr	Installer is trying to install new software. Type your password to allow this.	
⊖ Lice		puter.
🖯 Des	Name: Drew Shearman	on of
😑 Inst	Password:	All
Inst		
Sum	? Cancel Install Software	

-

6. Установка прошла успешно. Выберите Закрыть для выхода из программы установки. Рисунок 13: Установка прошла успешно.



7. FortiClient был сохранен в папку Applications. Рисунок 14: Папку Приложения.



8. Дважды щелкните FortiClient значок, чтобы запустить приложение. Выберите значок замка в левой нижней части приборной панели, чтобы внести изменения в FortiClient конфигурации.

Рисунок 15: Приборная панель по умолчанию заблокирована FortiClient.



Provisioning FortiClient

FortiClient конфигурации MSI инструмент

FortiClient конфигуратор инструментом является рекомендуемым методом создания индивидуальной установки FortiClient.

Использование

FortiClientConfigurator.exe-м <path к FortiClient.msi file>

[Необязательные параметры]

-М <path к FortiClient MSI файлу (обязательно)

- REGISTRATIONKEY <key>

Используйте для запретить пользователям изменять настройки FortiClient.

- FGTIP <ip:port или fqdn:port>

FortiClient попытается зарегистрируйтесь, чтобы получить эту FortiGate. Если он не может, он будет пытаться зарегистрироваться, чтобы по умолчанию шлюз.

Пример использования

FortiClientConfigurator.exe-MC: \ Downloads \ forticlient.msi

- REGISTRATIONKEY sercretpassword

Эта команда выше создает следующие каталоги, содержащие файлы готовые для развертывания:

C: \ Downloads \ FortiClient\_packaged \ ActiveDirectory \

C: \ Downloads \ FortiClient\_packaged \ ManualDistribution \

FortiClient конфигуратор

Инструмент FortiClientConfiguratorGUI это приложение, интерфейс к FortiClient переупаковка инструмент командной строки. Мастер проведет вас через процесс определения параметров, чтобы быть применяется к FortiClient файл MSI.

Этот документ был написан для FortiClient v5.0 Патч Release 1 для Windows. Не все функции описанное в этом документе поддерживаются для FortiClient v5.0 Патч Release 1

#### для Mac OS X. Выключатель и параметров чувствительны к регистру.

ĺ	🗱 Welcome 🛛 🗶
	Welcome to the FortiClient repackaging GUI. This is application is an interface to the FortiClient repackaging command-line tool.
	The wizard pages will take you through the process of specifying settings and customizations to be applied to the FortiClientdd MSI of your choice.
FortiClientConfig	
	< Back Next > Cancel

#### Рисунок 16: FortiClient интерфейс прикладного конфигурации.

Создание пользовательского файла установки MSI

Вы можете создать собственный файл установщика MSI для вашего специализированного приложение FortiClient:

1. Определите параметры командной строки, для этого нужно для установки настроенной FortiClient.

2. В папке, где вы расширили программу установки. ZIP пакета, выполните следующую команду линия запись:

FortiClientConfigurator.exe-м <path к FortiClient.msi file>

<optional switches>

Новый подкаталог создан, который содержит FortiClient файл MSI.

Развертывание FortiClient использованием Microsoft Active Directory (AD) сервер

Есть несколько способов установить FortiClient к конечной точке устройствами с помощью Microsoft Active

Directory.

Использование Microsoft AD развертывания FortiClient:

На контроллере домена, создайте точку распространения.

1. Войдите на сервер с учетной записью администратора.

Для получения дополнительной информации о конфигурации FortiClient XML см. в FortiClient v5.0 Справочник по XML

Fortinet на сайте технической документации, http://docs.fortinet.com.

Следующие инструкции основаны от Microsoft Windows Server 2008. Если вы используете различные версии сервера Microsoft, ваши или MMC оснастку в местах, могут быть различными.

2. Создание общей сетевой папке, где FortiClient файл установщика MSI будут распространяться с.

3. Установите права доступа к файлам на папку, разрешающие доступ к дистрибутиву. Скопируйте

FortiClient MSI пакет установки в эту общую папку.

4. Выберите Пуск> Администрирование> Active Directory пользователи и компьютеры.

5. После выбора домена, щелкните правой кнопкой мыши, чтобы выбрать новую организационную единицу (OU).

6. Перемещение всех компьютеров, которые необходимо распространять программное обеспечение для FortiClient вновь созданные подразделения.

7. Выберите Пуск> Администрирование> Управление групповой политикой. Групповая политика.

Управление оснастку откроется. Выберите OU вы только что создали. Щелкните правой кнопкой мыши, выберите Создание объекта групповой политики в этом домене и связать его здесь. Дайте новому GPO имя и нажмите OK.

8. Разверните объект групповой политики и найти контейнер групповой политики, который только что создали. Щелкните правой кнопкой мыши GPO и выберите Изменить. Редактор управления групповой политикой оснастку откроется.

9. Разверните узел Конфигурация компьютера> Политики> Параметры программ.

Щелкните правой кнопкой мыши Программное обеспечение

Настройки и выберите New> Package.

10.Выберите на пути к вашей точке распространения и FortiClient файл установки, а затем выберите Открыть. Выбор заданных и выберите ОК. Пакет будет создаваться.

11. Если вы хотите ускорить процесс установки, как на сервере и клиентских компьютерах, принудительно обновить GPO.

12. The программное обеспечение будет установлено на следующей перезагрузки клиентского компьютера. Можно также ожидать клиентском компьютере для опроса контроллера домена для изменения объекта групповой политики и установить программное обеспечение.

Удалите FortiClient использованием Microsoft Active Server каталогов

В этом разделе описывается, как удалить FortiClient с клиентских компьютеров с помощью Active Directory:

1. На контроллере домена, выберите Пуск> Администрирование> Управление групповой политикой.

Управление групповыми политиками оснастку откроется. Развернуть объектов групповой политики контейнер и щелкните правой кнопкой мыши объект групповой политики, созданный для установки и выберите FortiClient Изменить. Редактор управления групповой политикой откроется.

2. Выбор конфигурации компьютера> Политика> Настройки программы> Установка программного обеспечения. Вы будете теперь смогут увидеть пакет, который был использован для установки FortiClient.

3. Щелкните правой кнопкой мыши пакет, выберите Все задачи> Удалить. Выберите Немедленное удаление программное обеспечение от пользователей и компьютеров, или разрешить пользователям продолжать использовать программное обеспечение, но предотвращения новых установок. Нажмите кнопку ОК. Пакет будет удален.

4. Если вы хотите ускорить процесс удаления, как на сервере и клиентских компьютерах, заставить объект групповой политики обновления, как показано в предыдущем разделе. Программное обеспечение будет удалена со следующей перезагрузки компьютера. Можно также ожидать компьютер для опроса домен контроллера для изменения объекта групповой политики и удаления программного обеспечения.

Развертывание с помощью Microsoft System Center Configuration Manager 2007 Если вы хотели бы использовать системы от Microsoft Center Configuration Manager (SCCM) для развертывания FortiClient, используйте следующий метод:

Эти инструкции предполагают, у вас уже установлен и настроен SCCM. Если у вас нет, пожалуйста, обратитесь к Microsoft онлайн-источники справки для получения информации о выполнении этой задачи.

Шаг 1: создать пакет

1. Запуск вашей консоли Configuration Manager GUI и расширить следующее: Компьютер Управление> Программные пакеты дистрибутива>.

2. Щелкните правой кнопкой мыши и выберите пакеты Создать> Пакет из контекстного меню. Мастер открыть.

3. Заполните пакеты свойствами, как вы хотите на вкладке Общие.

4. На вкладке Источник данных выберите Этот пакет содержит исходные файлы коробку, а затем выберите Установить кнопку, чтобы указать источник SCCM пакет. SCCM попросит вас указать путь к исполняемый файл установки. Выбор этого пути, а затем выберите OK.

5. Установите флажок рядом с обновление точек распределения по расписанию, а затем установите планировать, как часто вы хотите.

6. Настроить параметры доступа к данным в случае необходимости.

7. На вкладке Параметры распространения, установить приоритет передачи. Высокая рекомендуется.

8. Под вкладку Отчетность, оставьте настройки по умолчанию.

9. Под вкладке Безопасность установить права для класса пакета и прав экземпляре.

10. Review ваш пакет выборы под вкладку Сводка, затем выберите Далее. Мастер завершить.

Шаг 2: Создание программы для вашего пакета.

1. Стартовая конфигурация вашего менеджера интерфейс консоли и раскройте следующие:

Управление компьютером > Распространение программного обеспечения> пакеты. Выберите только что созданную FortiClient пакета. Щелкните правой кнопкой мыши этот пакет и выберите Создать > Программа из контекстного меню.

2. На вкладке Общие, заполнить соответствующие подробности. Для автоматической установки, убедитесь, что вы использовать MS-переключатель под параметров командной строки.

3. На вкладке Требования установите флажки рядом с клиентских платформах вы хотите установить для (Windows Vista, Windows XP и т.д.).

4. Установите переменные окружения. Рекомендуется, чтобы выбрать, что программа могла работать.

5. Вы можете оставить Расширенный и Windows Installer вкладки по умолчанию.

6. Если вам требуется уведомление, направленное Microsoft Operations Manager (MOM), выберите соответствующие параметры на вкладке обслуживание.

7. Как и на предыдущем этапе, рассмотреть Ваше резюме, а затем создать вашу программу.

Шаг 3: реклама вашего пакета на клиентские компьютеры.

1. Стартовая конфигурация вашего менеджера интерфейс консоли и раскройте следующие:

Управление компьютером> Распространение программного обеспечения > Объявления. Щелкните правой кнопкой мыши и выберите Объявления Новое объявление > из контекстного меню.

2. При запросе нет распределительных пунктов, выберите Да. Мы будем обновлять распределения указывая позже в процессе.

3. По расписанию вкладке установите дату вы хотите. Установите уровень приоритета (рекомендуется установка "High"). Выберите на желтом звездочкой для указания обязательных параметров.

4. На вкладке Точки распространения, выберите "Загрузить содержимое с точки распространения и запустить локально как для все настроек.

5. При взаимодействии вкладке, вы можете использовать это, чтобы предупредить

зарегистрированным пользователям, что программа будет запустить и обеспечить таймер обратного отсчета до завершения исполнения.

6. Под вкладке Безопасность установить права для класса пакета и прав экземпляре.

7. Просмотрите выбранные параметры пакета под вкладку Сводка, затем выберите Далее. Мастер завершить.

Шаг 4: Создание и обновлять точки распространения

1. Стартовая конфигурация вашего менеджера интерфейс консоли и раскройте следующие:

Управление компьютером > Распространение программного обеспечения > пакеты. Расширен пакет, созданный и щелкните правой кнопкой мыши Точки распространения. Щелкните правой кнопкой мыши Точки распространения и выберите Создать точки распространения из контекстного меню. Откроется окно мастера.

2. Выберите SCCM сервер из списка доступных серверов и выберите Далее. Вы увидите резюме и мастера будет завершена.

3. Теперь вам необходимо обновить точки распространения, который был только что создан с пакета. Щелкните правой кнопкой мыши Точки распространения и теперь выбрать распространения обновлений

Очки из контекстного меню. Всплывающем окне появится. Подтвердите обновление, Да выбора.

# Использование Microsoft SCCM 2007 удалить FortiClient:

1. Откройте консоль Configuration Manager:

System Center Configuration Manager> База данных сайта> Управление компьютером> Распространение программного обеспечения> Пакет> Реклама.

2. Выберите FortiClient пакет, который вы хотите удалить, затем выберите для каждой системы удаления. Обеспечивать

выбран правильный коллекции границы. Укажите, когда реклама будет вещать членов целевой коллекции.

3. Завершите работу мастера. Убедитесь, что вы удалите начальные Реклама установке вы использовали для установки FortiClient для предотвращения SCCM от FortiClient переустановки.

#### Управление конечными точками

#### Введение

Целью этого раздела является предоставление базовой инструкции по настройки, развертывания и FortiClient управлять конфигурациями от FortiGate.

Настройка Управление конечными точками

В FortiOS v5.0, настройку и управление FortiClient агентов конечной точки теперь можно обрабатываются FortiGate. Можно настроить устройство FortiGate открыть для себя новые устройства сети, соблюдение FortiClient регистрации, и развернуть предварительно сконфигурированных конечной точке профиля подключенными устройствами. Конечная точка профиля могут быть развернуты на устройства в сети и более соединение VPN. Чтобы настроить Управление конечными точками на FortiGate, выполните действия, перечисленные ниже.

Шаг 1: Включить управление устройствами и трансляция сообщений обнаружения Для настройки устройства управления, выберите Система > Сетевой интерфейс>, выберите интерфейс, а выберите Правка на панели инструментов. На странице интерфейса редактирования можно по желанию включить обнаружение и идентификации устройств. Для включения трансляции сообщений обнаружения (опция) необходимо сначала включить FCT-Access под правами администратора. Нажмите кнопку Применить, чтобы сохранить настройки.

FortiOS Перевозчик GA v5.0.0 или более поздней версии.

Управление конечными точками доступно на FortiGate 40С и выше устройств.

Трансляция сообщений обнаружения является дополнительной конфигурации. При включении этой функции будет FortiGate рассылать сообщения компьютерной сети, позволяя клиентских подключений обнаружить FortiGate для FortiClient регистрации. Без эта функция включена, пользователь может ввести IP-адрес или адрес FortiGate для завершения регистрации.

E	Edit Interface
Name Alias Link Status	fmc1/2 (00:09:0F:DB:F2:55) Up
Addressing mode IP/Network Mask:	Manual DHCP Dedicate to FortiAP 187.28.154.2/255.255.255.0
Administrative Access	<ul> <li>✓ HTTPS</li> <li>✓ PING</li> <li>✓ HTTP</li> <li>✓ FMG-Access</li> <li>✓ SSH</li> <li>✓ SNMP</li> <li>✓ TELNET</li> <li>✓ FCT-Access</li> </ul>
Enable DHCP Server	
Security Mode Customize Portal Messages User Groups	Captive Portal  Click to add
Device Management Detect and Identify Devices Broadcast Discovery Messages	
Enable Explicit Web Proxy Listen for RADIUS Accounting Messages Secondary IP Address Comments	Write a comment 0/256
Administrative Status	í Up O © Down O
ОК	Cancel Apply

Рисунок 17: Параметры устройства управления

Шаг 2: Настройте клиентский профиль Endpoint

Чтобы настроить клиентский профиль Endpoint, Перейти к пользователю и устройства> Устройство> Endpoint профиля. Редактировать как требуется. Нажмите кнопку Применить, чтобы сохранить настройки.

Рисунок 18: конечная точка Редактировать профиль.

#### Edit Endpoint Profile

#### FortiClient Configuration Deployment

Wind	lows	and	Mac
------	------	-----	-----

AntiVirus Realtime Protection	n on Client (when installed)	
Application Firewall	client-reputation -	
Web Category Filtering	client-reputation -	
Disable Web Category Filteri	ng when protected by this FortiGate	
Endpoint Vulnerability Scan	on Client	
Schedule Scan Type:	💿 Daily 🖲 Weekly 🔘 Monthly	
🔽 Initiate Scan After Client Reg	jistration	
Client VPN Provisioning	O	
Name	Sunnyvale_California	
Туре	IPsec VPN	
Remote Gateway	12.2.43.1	
Authentication Method	Certificate 👻	
OFF Upload Logs to FortiAnalyze	r/FortiManager	
IP Address:	[Change]	
	Apply	

#### Шаг 3: Настройка политик брандмауэра

Чтобы настроить политику брандмауэра для Endpoint управления, перейдите в Политика > Политика. Политика > и выберите Создать новую на правой панели инструментов. Для политика Класс, выберите идентичность устройства.

Рисунок 19: Создание новой политики идентичности устройства.

	New Policy
Deline Tene	
Policy Type	• FIREWAIL VPN
Policy Subtype	🔘 Address 🔘 User Identity 🖲 Device Identity
Incoming Interface	internal 💌
Source Address	E Click to add
Outgoing Interface	wan1 👻
Enable NAT	
Ose Destination Interface Address	Fixed Port
Use Dynamic IP Pool	Click to add
Configure Authentication Rules	
😳 Create New 📝 Edit 👘 Delete	
Destination Address Device	Endpoint Compliance Service Schedule UTM Security Traffic Shaping Logging Action
	No matching entries found
Customize Authentication Messages	
Comments	Write a comment 0/255
	OK Cancel
1	

Добавить Примите аутентификации правило для всех совместимая с Windows-ПКклиентов. Это правило позволит Windows, клиенты, которые установили FortiClient и быть зарегистрированными на данной FortiGate к передачи трафика. Рисунок 20: принять правила для аутентификации совместимая с Windows-ПК-клиентов.

Destination Address	😑 all	•
Device	🛃 Windows PC	
Compliant with Endpoint Profile		
Schedule	🙋 always	-
Service	🚳 ALL	•
Action	✓ ACCEPT	-
Log Allowed Traffic		
Generate Logs when Session Starts		

Capture Packets

Добавить Captive Portal правила аутентификации для всех не-совместимая с Windows-ПКклиентов. Это правило перенаправления всех клиентов Windows (через веб-браузер) на специальный портал, где они могут скачать. После регистрации в FortiGate, конечная точка профиля будет назначена.

Рисунок 21: Пленница правила аутентификации портал для Windows-PC устройств.

Destination Address	🧧 all	0	
Device	🛃 Windows PC	0	
Schedule	🧧 always 👻		
Service	C ALL	0	
Action	Captive Portal		
Device Detection Portal			
Inforce FortiClient Compliance			
Email Address Collection			
Log Violation Traffic			

Traffic Shaping

(Необязательно) Добавьте правило Ассерt аутентификации, чтобы разрешить трафик от всех других устройств для передачи трафика без соблюдения FortiClient соответствия. Рисунок 22: Принять Правило проверки подлинности для всех других устройств.

Destination Address	all	<b>(</b> )
Device	All	
Compliant with Endpoint Profile		
Schedule	🔯 always	•
Service	Kall	
Action	✓ ACCEPT	
Log Allowed Traffic		

Как только эти три правила аутентификации настроен, выберите ОК, чтобы сохранить новые настройки политики.

Конфигурацию клиента готово к развертыванию. Рисунок 23: Политика брандмауэра конфигурации.

					ew Policy			
Policy Type		Firewall O VF	N.					
Policy Subtype		🔿 Address 🔿 U	ser Iden	ntity 💿 Dev	ice Identity			
Incoming Interface		any	any 👻					
Source Address		💽 all			0			
Outgoing Interface		port9 (Primary In	iternet)					
Enable NAT								
Configure Authen	tication Rules							
Create New	1 1.12 N Der	14 V	_					
Destination Addres	ss Device	Endpoint Compliance	Service	e Schedule	UTM Securit	y Traffic Shap	oing Logging	Action
	Windows PC	0	ALL	always	-	8	0	✓ ACCEPT
all								
all	Windows PC	0	ALL	always		0	0	O Captive Portal - Enforce FortiClient Compl
all	Windows PC All	0	ALL	always always	8	0	0	Captive Portal - Enforce FortiClient Comple
all all all	Windows PC All	0	ALL	always always	- 8	0	0	Captive Portal - Enforce FortiClient Compl     ✓ ACCEPT
all all all Customize Auth	Windows PC All ientication Messa	Ø Ø	ALL	always always	8	0	0	Captive Portal - Enforce FortiClient Compl     ✓ ACCEPT
aii all all Customize Auth Comments	Windows PC All rentication Messa	ages Write a commer	ALL ALL	always always	<b>8</b> #	0	0/255	Captive Portal - Enforce FortiClient Compl

После FortiGate конфигурация была завершена, вы можете приступить к FortiClient конфигурации. Настройте Windows PC в корпоративной сети со шлюзом по умолчанию установлены в IP из FortiGate.

FortiClient Endpoint топологии сети.

Следующий профиль FortiClient Endpoint топологий поддерживаются:

Клиент напрямую связано с FortiGate, либо к физическому порту, порту коммутатора или WiFi SSID.1

Эта топология регистрации клиента, настройка синхронизации и конечной точки профиля органов.

Клиент подключен к FortiGate, но находится за маршрутизатором NAT или device.2 Эта топология регистрации и настройки клиента синхронизации.

Клиент подключен к FortiGate через VPN connection.3

Эта топология регистрации клиента, настройка синхронизации и конечной точки профиля органов.

Рисунок 24: Топологии сети.



Чтобы настроить FortiClient Endpoint для управления, выполните действия, перечисленные ниже.

Шаг 1: Загрузите и установите FortiClient

Откройте веб-браузер на рабочей станции и попытка открыть веб-страницы, которая будет направлено на Captive Portal. Следуйте инструкциям на портале, чтобы загрузить и установить FortiClient.

Рисунок 25: Captive Portal блоке страницы отображается.

#### **Endpoint Security Required**

The use of this security policy requires that the latest FortiClient Endpoint Security software is working properly. Please make sure

- FortiClient is installed and running,
- FortiClient is registered with FortiGate and currently in "online" status, and the "Disable configuration sync with FortiGate" option in FortiClient settings is turned off.

Installing FortiClient requires that you have administrator privileges on your computer. If you do not, please contact your network administrator to have FortiClient installed.

The installer may be downloaded using the following link: FortiClientInstaller-Windows-Enterprise-5.0.0.exe

Installation instructions:

- For Internet Explorer:

  - Click the above link to download the installer
     When Internet Explorer asks what action you would like to take, click "Run"

• For Firefox:

- Click the above link to download the installer
   Save the installer and note the location it is saved to
- 3. Open the folder containing the installer and run it

FortiClient installation may take a few minutes. Thank you for your patience.

#### Шаг 2: FortiClient регистрации

После FortiClient завершает установку FortiClient запустится автоматически.

Устройство FortiGate для регистрации. Есть три способа, которыми FortiClient / FortiGate связи инициируется:

1. FortiClient подключается к предпочтительный IP-адрес (если имеется).

2. Если 1. не удается, FortiClient будет пытаться подключиться к IP-адрес шлюза по умолчанию.

3. Если 2. не удается, FortiClient будет ожидать FortiGate сообщений базовой станции. На рисунке 26 показан пример сообщения вещания прислал FortiGate и полученных FortiClient. Выберите Принять, чтобы зарегистрироваться в этом устройстве FortiGate. После регистрации FortiGate назначен Endpoint профиль FortiClient.

Рисунок 26: FortiGate широковещательное сообщение



Шлюз по умолчанию вашего персонального компьютера IP должны быть настроены на IP Set

FortiGate интерфейс.

Рисунок 27 показывает поведение FortiClient на первоначальной настройке. FortiClient выполнит поиск доступных.

K		ent iter is protected by FortiClient softwa	
	Searching for FortiGate	Searching for FortiGat	e Cancel
-	Remote Access	Weekly Scan at 18:	<u>30 on Monday</u>
Устройс <sup>а</sup>	Vulnerability Scan Vulnerability Scan Enabled гва FortiGate лля завег	Last Scan: Never Scanned	Last Update: 24/12/2012 Last Update Now OrtiGate значок на

приборной панели, чтобы повторить поиск. Рисунок 27: FortiClient будет искать доступные FortiGate.

FortiClie This compu	ent ter is protected by FortiClient software
Searching for FortiGate	Searching for FortiGate
Remote Access	Weekly Scan at 18:30 on Monday
Vulnerability Scan Vulnerability Scan Enabled	Last Scan: Never Scanned Last Update: 24/12/2012

Если FortiClient не может обнаружить устройство FortiGate, введите IP-адрес или URL устройства и выберите кнопку Повторить, как показано на рисунке 28. Рисунок 28: Введите FortiGate IP или URL

FortiClient This computer	IS protected by FortiClient software
FortiGate Not Found	
For E	tiGate Not Found. Specify FortiGate IP or URL Retry Don't Register
Remote Access	Weekly Scan at 18:30 on Monday
Vulnerability Scan	Last Scan: Never Scanned Last Update: 24/12/2012       Scan Now      Update Now

Когда FortiClient находит FortiGate, вам будет предложено подтвердить регистрацию в как показано на рисунке 29. Нажмите кнопку Подтвердить для завершения регистрации. Рисунок 29: Подтверждение регистрации окна.

Registering to FortiGate: 192.168.10.1(FWF60C3G11011606) With following information Endpoint User: punky Logged into Domain: Hostname: spirit	FURTINET
Confirm	Cancel

После успешной регистрации, FortiGate развернет конфигурации конечной точки. Рисунок 30: Регистрация завершена.



Шаг 3: FortiGate развертывает Endpoint профиля FortiGate развернет Endpoint после завершения регистрации. Профиль позволит трафик через FortiGate. Значёк системном трее появится.

Рисунок 31: Настройка уведомлений об обновлениях сообщение.



FortiClient консоли будет отображаться, что она успешно зарегистрирован в FortiGate. Endpoint профиля устанавливается на FortiClient.

Рисунок 32: Зарегистрированные консоли FortiClient.



Развертывание Endpoint профиля с клиентами через VPN

Можно развернуть Endpoint профиль клиентам через соединение VPN.

1. На приборной панели FortiGate, выберите Настройки> File. При регистрации выберите Указать FortiGate-адрес и введите IP-адрес и номер порта (если необходимо) в FortiGate

Внутренний интерфейс. Рисунок 33: Предпочтительный адрес FortiGate.

<ul> <li>Registration</li> </ul>	
Specify FortiGate address	
✓ Default gateway	
✓ Listen for broadcast messages	

2. Настройка соединения IPsec VPN от FortiClient к управлению FortiGate. Для получения дополнительной информация о настройке IPsec VPN см. раздел «Создание нового IPsec VPN соединения".

3. Подключение к VPN.

4. Теперь вы можете искать для FortiGate шлюз. См. "Шаг 2: FortiClient регистрация" для получения дополнительной информации.

5. После регистрации, клиент имеет возможность получить Endpoint профиля. Fortinet Технологии Инк

FortiClient v5.0 Патч Release 1 добавляет возможность помнить при принятии FortiGate транслироваться сообщение о регистрации.

Рисунок 34: Вариант помнить FortiGate.

d 📃 📉
A broadcast registration message received from FortiGate 172.17.61.169 (FG80CM3909613127).

Выберите значок Регистрация на приборной панели для просмотра информации о текущем зарегистрированных

устройства, включая имя компьютера, домен, серийный номер и IP-адреса. Рисунок

35

FortiClient	F#RTINET.
Registered to Forti	Gate FG80CM3909613127
AntiVirus Real-time Protection Enabled	Registered (Online) Hostname: Win7-64-PC Domain: N/A
Web Filter Protected by Fortigate	IPSe     SN: FG80CM3909613127       IP: 172.17.61.169       Remembered FortiGates         Unregister
Application Firewall Application Firewall Enabled	Password
Remote Access	
Vulnerability Scan Vulnerability Scan Enabled	Connect

Эта функция будет улучшена в будущих выпусках патч, чтобы FortiClient для автоматического переключения между различными устройствами запоминающийся. Выберите список устройств FortiGate, что имеет FortiClient paнee зарегистрированных. Вы также можете изменить порядок устройств в этом списке с помощью контекстного меню.

Рисунок 36: Показать устройств.

Remembered FortiGates	Last Seen
FW81CM3912600092 FW81CM3912600092:172.17.61.87	2013-00-08 17:26:07
FG200B3910601483 FG200B3910601483:172.17.61.14	2013-00-08 17:26:53 Forget
FG80CM3909613127 FG80CM3909613127:172.17.61.169	Move up 1/5 2013-00-08 17:29:15
Save	Close

Посмотреть FortiClient регистрации на веб-FortiGate-администратора Вы можете просмотреть все FortiClient зарегистрированных на FortiGate вебадминистратора. В каждом новом регистрация будет автоматически добавляться в таблице устройств. Для просмотра зарегистрированных устройств Пользователь & Устройства > Устройство > определение устройства. Рисунок 37: Устройство FortiGate.

Device	05	User	Hostname	IP Address	Custom Group	FortiClient State	Last Seen
Manufacture of		Administrator	chris-9958239c0	192.168.12.201	the second s	() NA	11 seconds ago (intern
Device Detail	and the second			192.168.10.1		© N/A	Friday (wan1)
Device	6 b4:99:ba:f7:ca:Sc		WIN-CI9P9G6D7U2	172.17.61.214		O N/A	Friday (wan1)
05	Windows / 7 (x64)			172.17.61.64		O N/A	Friday (wan1)
Hostname	spirit			172.17.61.140		© N/A	8 seconds ago (wan1)
Username	punky			172.17.61.60		O N/A	40 seconds ago (wan1
IP Address	192.168.10.111	Summer		172.17.61.49		O NA	34 minutes ago (want)
Last Seen	Seen 1 second ago (internal) iClient 😵 Registered (default)	ET de	QA-PC1	192.168.10.205		Blocked/Captive Portal	1 second ago (internal
East Seen				172.17.61.17		O NA	3 minutes ago (wan1)
State				172.17.61.45		() N/A	14 minutes ago (want)
- Charles		- Children (* 1970)		172.17.61.42		O N/A	8 minutes ago (wan1)
27 b4:99:ba:f7:c	18:5c Windows / 7 (x64)	punky	apirit	192.168.10.111	1 8	Registered (default)	1 second ego (internal
d4:be:d9:d8:	de:57		Hong-PC-163	192.168.10.201		O N/A	3 hours ago (internal)
00:40:f4:91:e0:c2		[] jinhai	JONHAIWIN7-64			O N/A	1

Настроить IP предпочтительным FortiGate на FortiClient для регистрации FortiClient пользователя администратор может указать предпочтительный FortiGate IP адрес для регистрации и управление конфигурации клиента. Когда незарегистрированной FortiClient запускается, он сначала ищет предпочтитаемым FortiGate. Если предпочтительный FortiGate недоступен, она будет выглядеть для подключения к шлюз по умолчанию. Если оба предпочтительным FortiGate и шлюз по умолчанию не доступны, FortiClient будет принимать широковещательное сообщение от FortiGate. Чтобы настроить предпочтительный FortiGate IP адрес на FortiClient, перейдите в меню Файл > Настройки. Выбирать

Регистрация расширить выпадающее меню. Введите IP-адрес и номер порта (если требуется) внутреннего интерфейса FortiGate автора.

Рисунок 38: Настройка предпочтительного FortiGate на FortiClient

Registration	
Specify FortiGate address	
✓ Default gateway	
✓ Listen for broadcast messages	

Включить FortiClient Endpoint регистрации (опционально)

Чтобы включить FortiClient Endpoint. Регистрация на FortiClient, выберите Система> Конфигурация> Дополнительно.

Выберите Включить ключ регистрации на FortiClient, ввести регистрационный ключ и выберите Применить.

Рисунок 39: Включить FortiClient Endpoint Регистрация на FortiGate.

#### FortiClient Endpoint Registration

👿 Enable Registration Key for I	FortiClient	
Registration Key	•••••	
		Apply

FortiClient пользователю нужно будет ввести тот же регистрационный ключ для успешной peruстрации FortiClient к FortiGate.

# Антивирус

FortiClient Antivirus

FortiClient v5.0 включает в себя модуль антивирус для сканирования системных файлов, исполняемых файлов, DLL. FortiClient также поиска и удаления руткитов.

В этом разделе описывается, как включить антивирус и параметров конфигурации.

#### Включить / отключить антивирус

Чтобы включить или отключить FortiClient защита в реальном времени, переключите [Enable / Disable] в меню FortiClient приборной панели.

#### Уведомления

Выберите FortiClient приборной панели, чтобы просмотреть все уведомления. Когда вирус был обнаружен, восклицательный появится значок антивируса в дереве меню вкладки. Значок изменится с серого на желтый. Выберите Все, чтобы просмотреть все уведомления Antivirus события.

Рисунок 40: Уведомления окна.

FortiClient This computer is	FERTINET.
AntiVirus 5 Threats Quarantined	Notifications     close       Real-ti     AntiVirus: Malware:EICAR_TEST_FILE i       Databi     24/12/2012 3:19:16 PM
Parental Control Parental Control Enabled	5 Three
Application Firewall Application Firewall Enabled	View All Exclusion List
Remote Access	Weekly Scan at 18:30 on Monday
Vulnerability Scan Vulnerability Scan Enabled	Last Scan: Never Scanned Last Update: 24/12/2012

### Scan Now

Для выполнения сканирования по требованию антивируса, выберите кнопку Scan Now на FortiClient приборной панели. В раскрывающемся меню выбрать вариант Выборочная проверка, Полная проверка, Быстрая проверка.

Приборная панель отмечает дату последнего сканирования выше кнопки.

Выборочное сканирование работает двигатель обнаружения руткитов для обнаружения и удаления руткитов. Выборочное сканирование позволяет выбрать определенную папку, файл на вашем локальном жестком диске (HDD) для сканирования на наличие угроз. Полная проверка запускается двигатель обнаружения руткитов для обнаружения и удаления руткитов. Полное сканирование затем выполняет полную проверку системы, включая все файлы, исполняемые файлы, библиотеки DLL и драйверы для угроз. Быстрое сканирование системы запускает двигатель обнаружения руткитов для обнаружения обнаружения и удаления все файлы, исполняемые файлы, библиотеки DLL и драйверы для угроз.

Быстрое сканирования проверяет только исполняемые файлы, DLL, драйверы, которые в настоящее время работают на наличие угроз.

Рисунок 41: Антивирусный сканирующий варианты.

FortiClient	FEIRTINET
This computer is	s protected by FortiClient software
AntiVirus 5 Threats Quarantined	Real-time Protection Enabled [Disable] Database is up-to-date
Parental Control Parental Control Enabled	5 Threats Quarantined
Application Firewall Application Firewall Enabled	Exclusion List
Remote Access	Quick Scan Full Scan
Vulnerability Scan Vulnerability Scan Enabled	Custom Scan     Last Update: 24/12/2012       Scan Now     Update Now

Проверить файл или папку. Чтобы выполнить проверку на вирусы определенного файла или папки, щелкните правой кнопкой мыши файл которую необходимо поверить и нажмите Проверить.

D 40	0	1	1 U
Pucyhok $\Delta f$	Сканирование	определенного ф	фаида или папки
1  MC ymort + 2.	CRaimpobaline	определенного ч	parina riniri manteri.

		Open	
		Browse in Adobe Bridge CS5.1	
2012 TBD -		Share with	+
	$\odot$	MagicISO	•
	8	SVN Checkout	
	-	TortoiseSVN	•
		Add to archive	
		Add to "•• 2012 TBD ••.rar"	
<b>C</b>		Compress and email	
FortiClient		Compress to "•• 2012 TBD ••.rar" and email	
	9	ZipGenius	•
		Restore previous versions	
	饧	Combine supported files in Acrobat	
A M		Create ISO image file	
	3	Scan with FortiClient AntiVirus	

FortiClient S	Scan Progress
	FortiClient
Scanning for viru	uses and malware
Action: Location: Item: Scanned files: Infected files:	Scan files         C:\Users\dshearman\Desktop\SVN Updates\SVN FCT\31         31de06333609d5297764dc05a545efc7c80036c3.svn-base         24       Scanned boot blocks:         0       Infected boot blocks:
	Pause Stop Show Details >>

#### Обновить сейчас

Для выполнения по требованию обновление FortiClient версии, двигатели, а также подписи, выберите Обновить сейчас кнопку на панели содержимого. Содержание области заметок дате последнего обновления выше кнопки.

Для просмотра текущей версии FortiClient, двигатель, и подпись информацию, выберите Справка в панели инструментов на выпадающее меню.

Рисунок 43: FortiClient страницы.

<b>FortiClient</b> 5.0.1.194 (latest version)			Quick Start Guide
Serial:		FCT8001381786725	
UID2:		BE6B76C509DB4CF	3A8CB942AED2064A0
Engine		Status	Version
AntiVirus:	<ul> <li>Image: A start of the start of</li></ul>	Up-to-date	5.035
Anti-Rootkit:	$\checkmark$	Up-to-date	2.025
Signatures		Status	Version
AntiVirus:	<ul> <li>Image: A start of the start of</li></ul>	Up-to-date	16.909
AntiVirus Extended:	$\checkmark$	Up-to-date	16.866
Anti-Rootkit:	$\checkmark$	Up-to-date	1.546
Application:	$\checkmark$	Up-to-date	4.277
Vulnerability Scan:	$\checkmark$	Up-to-date	1.292
			Copyright Information
		Close	

#### Расписание Антивирусная проверка

Чтобы запланировать антивирусное сканирование, выберите еженедельного осмотра на панели содержимого. В этом меню вы можете настроить параметры, описанные в

#### следующих рисунков и таблиц. Рисунок 44: Antivirus планирования.

File Help	
Configure	the AntiVirus Scan Schedule
Schedule Type Scan On Start Scan Type	Weekly Monday 18 I 30 I (HH:MM) Full system scan
	DK Cancel

#### Тип расписания

Выберите ежедневно, еженедельно или ежемесячно в выпадающем меню. Сканирование.

Для еженедельного сканирования по расписанию, выберите день недели на

раскрывающегося меню. Ежемесячные проверки по расписанию, день месяца, на раскрывающегося меню.

#### Начало

Выберите время начала на выпадающее меню. Формат времени:

представлены в часах и минутах, 24-часовом формате.

#### Тип сканирования

Выберите тип сканирования:

Выборочное сканирование работает двигатель обнаружения руткитов для обнаружения и удаления руткитов. Выборочная проверка позволяет выбрать определенную папку файл на вашем локальном жестком диске (HDD) для сканирования на наличие угроз.

Полная проверка запускается двигатель обнаружения руткитов для обнаружения и удаления руткитов. Полная проверка выполняет полное сканирование системы, включая все файлы, исполняемые файлы, DLL, и драйверами для угроз.

Быстрое сканирование системы запускает двигатель обнаружения руткитов для обнаружения и удаления руткитов. Быстрое сканирование системы только проверяет исполняемые файлы, DLL, драйверы, которые в настоящее время работают на наличие угроз.

#### Посмотреть карантин угрозы

Для просмотра карантин угроз, выберите раздел Угрозы карантине на FortiClient приборной панели. На этой странице вы можете просмотреть, восстановить или удалить

файл из карантина.	Вы также может	те отправить	файл в	FortiGuard.
Рисунок 45: Угрозы	і карантин стран	ицы		

	File Name	Date Quarantined			
1	e3cngriy.com.part 2012/12/24 15:18:32				
	juh3vugh.com.part	2012/12/24 15:18:32			
	bsqzdhta.com.part	2012/12/24 15:18:33			
	ce3v4tze.com.part	2012/12/24 15:18:33			
	uavbtna3.co Submit v	irus and a second s			
	Sending file Infected file: C:\Program Files (x86)\Fortinet\FortiClient\quarantFile22835e6f Griginal Original Out				
	Submitted Not Submitted				
Status		Quarantined			
	Virus Name	EICAR_TEST_FILE			
	Quarantined File Name	QuarantFile22835e8f			
	Logs Refresh Submit Restore Delete Close				

Имя файла.

Дату и время, когда файл был помещен на карантин FortiClient.

Информация о файле. Выберите файл из списка, чтобы просмотреть подробную информацию, включая карантин, статус, имя вируса и помещенных в карантин имя файла.

Журналы. Выберите для просмотра FortiClient данных журнала.

Обновление. Выберите, чтобы обновить список.

Представлять. Выберите представить файл на карантине FortiGuard.

Восстановление. Выберите, чтобы добавить выбранный файл / папку в список исключений.

Удалять. Выберите для удаления файла в карантине.

Близко. Выберите, чтобы закрыть страницу и вернуться к FortiClient приборной панели. Для добавления файлов / папок в список исключений антивируса, выберите Список исключений на панели содержимого. На следующие страницы конфигурации, выберите

символ '+', чтобы добавить файлы или папки в список. Любые файлы

или папки на этом список исключений не будет проверяться.

Рисунок 46: Список исключений антивируса

Exclusion List	
Add file/folder to the exclusion list	
C:\Users\dshearman\Desktop\Technical Documentation	~
OK Canad	

#### Antivirus предупреждение

Когда FortiClient антивирус обнаруживает вирус при попытке скачать файл через веббраузер, Вы получите сообщение предупреждающий диалог как на рисунке 47. Перейдите в карантин угрозы на приборной панели, чтобы просмотреть сведения об обнаружении угрозы.

Рисунок 47: Пример вируса предупреждение

Virus Ale	rt	x
	Process: Item:	C:\Program Files (x86)\Mozilla Firefox\firefox.exe c:\users\dshearman\appdata\local\temp\1twzq+gg.com.part
	Virus:	EICAR_TEST_FILE
	Status:	Quarantined
Cl	not show me ose v recently det	this alert for next 24 hours ected virus(es)

# Antivirus регистрации

Чтобы настроить антивирусную лесозаготовки, выберите Файл на панели инструментов и настройки на выпадающее меню. Выберите вход, чтобы посмотреть в выпадающем меню.

В этом меню вы можете настроить вариантов, изложенных на следующем рисунке. Рисунок 48: Вход варианты.

	~	· · · 1						
Enable logging for these features: VPN Application Firewall AntiVirus Parental Control Update Vulnerability Scan Log Level Information Log file Export logs Clear logs	▼ Lo	▼ Logging						
Important       AntiVirus       Parental Control         Update       Vulnerability Scan         Log Level       Information         Log file       Export logs		Enable logging fo	r these features:	VPN	Application Firewall			
Update     Vulnerability Scan       Log Level     Information       Log file     Export logs				🔽 AntiVirus	Parental Control			
Log Level     Information       Log file     Export logs				🔲 Update	Vulnerability Scan			
Log file <u>Export logs</u> <u>Clear logs</u>		Log Level	Information					
		Log file	Export logs Clear lo	ogs				

Активируйте функцию ведения эти функции

Выберите антивирусную включить ведение журнала для этой функции.

Уровень Журнала

Выберите уровень регистрации:

Авария: система становится нестабильной.

Alert: требуются незамедлительные действия.

Критические: Функциональность влияет.

Ошибка: ошибка существует и функциональность может быть затронуто.

Предупреждение: функциональность может быть затронуто.

Примечание: Информация о нормальных событий.

Информация: Общие сведения о системе операций.

Debug: Debug FortiClient.

Лог-файл

Экспорт журналов. Выберите для экспорта журналов на локальном жестком диске (HDD) Журнал формат.

Очистить журналы. Выберите, чтобы очистить все журналы. Вы увидите окно подтверждения, выберите Да, чтобы продолжить.

## Параметры антивируса

Чтобы настроить параметры антивируса, выберите Файл на панели инструментов, и настройки на выпадающее меню. Выберите параметры антивируса, чтобы посмотреть в выпадающем меню. В этом меню вы можете настроить параметры изложенным в следующих рисунков и таблиц.

Рисунок 49: параметры антивируса.

AntiVirus Options

Grayware Options

🔽 Adware 📝 Riskware

Alert when viruses are detected

Pause background scanning on battery power

Enable FortiGuard Analytics

#### Параметры антивируса

Опции нежелательных программ

Нежелательных программ это зонтичный термин применяется к широкому кругу Вредоносные программы, такие как шпионское, рекламное ПО и ключевые лесорубов, которые часто тайно установленных на компьютере пользователя, чтобы отслеживать и / или сообщать определенную информацию обратно на внешнее источника без разрешения пользователя или знаний.

Выберите, чтобы включить обнаружение рекламного и карантина в течение антивирусное сканирование.

Потенциально опасные программы. Выберите, чтобы включить обнаружение потенциально опасных программ в течение антивирусное сканирование.

Сигнал тревога когда вирусы обнаружены.

Выберите для FortiClient направлять уведомление, когда

обнаружении угрозы на вашем персональном компьютере.

Пауза фоне сканирования от батареи.

Выберите, чтобы приостановить фоновое сканирование, когда ваши личные компьютер работает от батареи.

Включить FortiGuard Analytics Выберите для автоматической отправки подозрительных файлов в FortiGuard

# FortiClient Родительский контроль / веб-фильтрации

Родительский контроль / Веб-фильтрация позволяет блокировать, позволяют, предупреждают и мониторинга веб-трафика на основе URL на категорию. URL категоризации обрабатывается FortiGuard Сети.

Включить / отключить Родительский контроль / веб-фильтрации

Чтобы включить или отключить Родительский контроль FortiClient / Веб-фильтрация, переключите [Enable / Disable]

кнопки на приборной панели FortiClient. Родительский контроль включен по умолчанию. Рисунок 50: модуль Родительский контроль.



Когда FortiClient зарегистрирован в FortiGate, модуль Родительский контроль будет отражать веб- фильтрация. Вы можете отключить веб-фильтрации на FortiClient от FortiGate. Устройство находится за FortiGate, клиентское устройство будет использовать Web Filter профиль на FortiGate.

Включить / Выключить

Переключите для включения или отключения функции родительского контроля. Настройки.

Выберите вариант настройки профиля Родительского контроля.

Родительский контроль / Web параметров фильтрации

Вы можете настроить профиль разрешать, блокировать, предупредить или мониторинга веб-трафика на основе категории Профиль. Используйте меню правой кнопкой мыши, чтобы установить меры для полного категорию или подкатегорию.

Вы можете добавлять сайты в список исключений и установить разрешение, разрешить или запретить. Если сайт является частью заблокированного категории, позволяющие разрешение в списке исключений позволит

пользователю получить доступ к конкретным URL.

Рисунок 51: Профиль и список исключений.

File Help

Profile			Exclusion List
<ul> <li>Adult/Mature Content</li> <li>Abortion</li> </ul>		The following	web sites are explicitly blocked or allowed
🔲 🥥 Advocacy Organizations		Permission	URL
		0	www.facebook.com
		0	www.fortinet.com
Alternative Poliofe		0	www.penthouse.com
<ul> <li>Dating</li> <li>Gambling</li> <li>Gambling</li> <li>Lingerie at monitor</li> <li>Marijuana</li> <li>Nudity and Risque</li> <li>Other Adult Materials</li> <li>Pomography</li> </ul>	Ŧ	+ - 2	



Посмотреть профиль нарушений

Для просмотра профиля нарушений, выберите правонарушениях (в течение последних 7 дней) на FortiClient приборной панели.

Рисунок 52: Нарушения правил дорожного движения.

Website	Category	Time	User
ffupdate.conduit-services.com	Malicious Websites	25/10/2012 9:53:37 AM	dshearman

# **Application Firewall**

FortiClient Применение межсетевого экрана

FortiClient v5.0 может распознавать трафик, генерируемый большое количество приложений. Вы можете создавать правила для блокировки или разрешения этого трафика в каждой категории, или приложение.

В этом разделе описывается, как включить настройки Application Firewall.

Включение / выключение Application Firewall

Чтобы включить или отключить FortiClient защита в реальном времени, выберите [Enable / Disable] на пульте FortiClient приборной панели.

Рисунок 53: Модуль Application Firewall.



# Посмотреть Блокировка приложений

Для просмотра блокированных приложений, выберите Блокировка приложений на приборной панели FortiClient странице перечислены все приложения заблокированы в последние семь дней, в том числе количество и время последнего запуска.

Правила Application Firewall

Для просмотра правил Application Firewall, выберите Настройки на FortiClient приборной панели.

Рисунок 54: Правила Application Firewall.

Add Rule	
Application/Category	Action
FortiClient (Other)	0
Botnet	0
iTunes (Apple)	0

Чтобы добавить новое правило 1. Нажмите кнопку Добавить правило. Рисунок 55: Окно добавления правила.

🔘 Ca	ategory	Applic	ation	
Face	ebook (F	acebook	)	0
Actio	n:	Block		
		Allow		
Place	ement:	At the t	ор	
		At the I	oottom	
		DK	Cance	

Fortinet Технологии Инк

2. Выберите любой из этих категорий или приложения. Для категории, используйте выпадающий список для выбора категории. Для приложений, типа поставьте полное имя

приложения или первую букву для поиска.

Все приложения, начиная с выбранного письма.

3. Выберите действие, блокировать или разрешать категорию или приложения.

4. Выберите размещение правило в верхней или в нижней части.

5. Нажмите ОК, чтобы сохранить настройки.

Чтобы изменить правило

1. На странице настроек, при наведении курсора мыши на правило, скрытое меню значок доступны.

2. Выберите значок редактирования, чтобы изменить действие для правила.

3. Выберите значок удаления, чтобы удалить правило.

4. Выберите значок перемещения и перетащите и падение правило в новое положение в списке.

5. Нажмите ОК для сохранения настроек и возврата в FortiClient приборной панели. Logging Application Firewall

Для настройки ведения журнала Application Firewall, выберите Файл на панели инструментов, и настройки на раскрывающегося меню. Выберите вход, чтобы посмотреть в выпадающем меню. Выберите Application Firewall вход меню позволяет включить ведение журнала для этого модуля.

FortiClient Firewall приложение может блокировать приложения, для которых имеет FortiGuard

Приложение подпись. Вы можете отправить запрос на добавление приложений на подпись FortiGuard сайта.

IPsec VPN и SSL-VPN

FortiClient удаленного доступа (VPN)

FortiClient v5.0 поддерживает как IPsec и SSL VPN-подключения к сети для удаленного доступа.

В этом разделе описывается, как настроить удаленный доступ.

Добавить новое подключение

Выберите пункт Настройка VPN на приборной панели, чтобы FortiClient добавления новой конфигурации VPN.

Рисунок 56: Настройка нового подключения VPN.



Создайте новый SSL-VPN соединение

Для создания нового SSL-VPN соединение, выберите Настройка VPN или использовать выпадающее меню на приборной панели. В этом меню вы можете настроить параметры, описанные в следующих рисунков и таблиц.

Рисунок 57: SSL-VPN параметры конфигурации.

Connection Name	ssl_90_1
Туре	SSL-VPN 🔘 IPsec VPN
Description	
Remote Gateway	10.10.90.1;ssldemo.fortinet.com
	Customize port 443
Authentication	Prompt on login
	Save login
Username	test
Client Certificate	
Certificate	[Prompt on connect]
Do not Warn Invalid Server Certificate	
	OK Cancel

Тип Выберите SSL-VPN.

Описание

Введите описание для соединения. (Опционально)

Шлюз удаленных

Введите IP адрес / имя хоста удаленного шлюза. Несколько удаленных

Шлюзы могут быть настроены, разделяя записи точкой с запятой.

Если шлюз не доступен, VPN будут подключаться к следующему

настроить шлюз.

Порт

Выберите для изменения порта. По умолчанию используется порт 443.

Идентификация

Выберите для ввода при входе в систему, или запомнить.

Имя пользователя

Если вы выбрали для сохранения входа, введите имя пользователя в диалоговом окне. Сертификат клиента

Выберите, чтобы включить клиентские сертификаты.

Сертификат

Выберите сертификат опцию выпадающего меню.

Не предупреждать Неверный

Сертификат сервера

Выберите, если вы не хотите, чтобы предупредил, что если сервер представляет

недействительным

сертификат.

Создайте новый IPsec VPN соединения

Для создания нового IPsec VPN соединение, выберите Настройка VPN или использовать выпадающее меню на GUI. В этом меню вы можете настроить параметры, описанные в следующих рисунков и таблиц.

Рисунок 58: IPsec VPN параметров конфигурации.

Cri	eate new VPN Connection
Connection Name	psk_90_1
Туре	SSL-VPN ( IPsec VPN
Description	
Remote Gateway	10.10.90.1; ipsecdemo.fortinet.com
Authentication Method	Pre-Shared Key
Pre-Shared Key	•••••
Authentication (XAuth)	<ul> <li>Prompt on login</li> <li>Save login</li> </ul>
Username	test
	OK Cancel
Имя соединения Введите имя для соединения. Тип	
Выберите IPsec VPN.	
Описание Ввелите описание лля соелинения (	Опционально)
Шлюз удаленных	
$\mathbf{P}_{\mathbf{P}}$ алита IP алиас / имя хоста улалани	

Введите IP адрес / имя хоста удаленного шлюза. Несколько удаленных Шлюзы могут быть настроены, разделяя записи точкой с запятой.

Если шлюз не доступен, VPN будут подключаться к следующему

настроить шлюз.

Идентификация

Метод

Выберите либо сертификатов Х.509 или общий ключ на раскрывающийся меню.

Сертификат Х.509,

Предварительный ключ

Выберите Сертификат Х.509 на выпадающее меню, или введите предварительный ключ в диалоговом окне. См. сертификат управления для

информация о настройке Параметры сертификата.

Идентификация

(XAuth)

Выберите для ввода при входе в систему, запомнить, или отключить.

Имя пользователя

Если вы выбрали Сохранить логин, введите имя пользователя в диалоговом окне. Подключение к VPN

Для подключения к VPN, выберите имя VPN из выпадающего меню. Введите имя пользователя, пароль и выберите кнопку Подключить.

Рисунок 59: Варианты

подключения.

(	FortiClient This computer is	protected by FortiClient software	Fiirtinet.
0	AntiVirus 5 Threats Quarantined		
		🖵 psk 90 1	- 66.
Ŵ	Parental Control Parental Control Enabled	Add	a new connection the selected connection
	Application Firewall Application Firewall Enabled	Password	te the selected connection
₽	Remote Access No VPN Connected		
	Vulnerability Scan Vulnerability Scan Enabled	Connect	

Вы можете также выбрать параметры для существующего соединения VPN и удалить существующее соединение VPN с помощью выпадающего меню.

При подключении, приборная панель будет отображать состояние подключения, продолжительность и другие соответствующие информации. Теперь вы можете просматривать ваши отдаленные сети. Выберите кнопку Отключить, когда вы готовы завершить сеанс VPN.

Рисунок 60: SSL-VPN соединение, установленное.

FortiClien	t	F©RTINET.
This computer	is protected by FortiClient softwa	are 😰   ݤ
AntiVirus Realtime Protection Enabled	VPN Name demo site	
Parental Control	Status	🗿 Up
	Duration	O0:00:24
Application Firewall Application Firewall Enabled	Bytes Received	⇔ 4331
	Bytes Sent	⇒] 8279
Remote Access		
Vulnerability Scan Vulnerability Scan Enabled	Discon	nect
Расширенные функции (Windows Соединение VPN перед входом в VPN <options> тег содержит глоб будет подключения, а затем вход <forticlient_configuration></forticlient_configuration></options>	s) систему (AD средах) бальную информацию управлен в систему к AD / домен.	ия VPN государств. VPN
<vpn></vpn>		
<pre><show_vpn_before_logon> 1 <!-- sho<br--><use_windows_credentials> 1 <!-- us<br--><!-- Функции--></use_windows_credentials></show_vpn_before_logon></pre>	ow_vpn_before_logon> se_windows_credentials>	

</ VPN> </ Forticlient\_configuration> Статус Состояние соединения VPN. Продолжительность Продолжительность соединения VPN. Получено байт Байт получено через соединение VPN. Отправлено байт Байты, посланные через соединение VPN. Fortinet Технологии Инк Создания избыточного IPsec VPN Для использования VPN отказоустойчивости / резервирования, вы будете настроить список серверов FortiGate IP / FQDN, вместо одного: <forticlient\_configuration> <vpn>

```
<ipsecvpn>
<options>
</ Функции>
<connections>
<connection>
<name> psk_90_1 </ Name>
<type> руководства </ Туре>
<ike settings>
<prompt_certificate> 0 </ prompt_certificate>
<server> 10.10.90.1; ipsecdemo.fortinet.com; 172.17.61
0.143 < cepbep>
<redundantsortmethod> 1 </ redundantsortmethod>
•••
</ Ike_settings>
</ Связь>
</ Подключения>
</ Ipsecvpn>
</ VPN>
</ Forticlient configuration>
Это сбалансированная, но неполное XML фрагмент конфигурации. Все закрывающие теги
включены, но некоторые важные элементы для завершения конфигурации IPsec VPN,
опушены.
RedundantSortMethod = 1
Этот тег XML устанавливает соединение IPsec VPN, как пинг-ответ, основанный. VPN
будут подключаться к FortiGate который отвечает самым быстрым.
RedundantSortMethod = 0
По умолчанию RedundantSortMethod = 0, и соединение IPsec VPN является приоритет,
основанный. Приоритет конфигурации на основе будет пытаться подключиться к
FortiGate начиная с первой в списке.
Приоритет, основанный SSL-VPN соединений
SSL-VPN поддерживает конфигурации на основе приоритета для избыточности.
<forticlient configuration>
<vpn>
<sslvpn>
<options>
<enabled> 1 </ включен>
</ Функции>
<connections>
<connection>
Fortinet Технологии Инк
Страница 54
FortiClient v5.0 Руководство администратора
<name> ssl_90_1 </ Name>
<server> 10.10.90.1; ssldemo.fortinet.com; 172.17.61.143:44
3 </ сервер>
•••
</ Связь>
</Полключения>
</ SSLVPN>
</ VPN>
```

```
</ Forticlient configuration>
Это сбалансированная, но неполное XML фрагмент конфигурации. Все закрывающие теги
включены, но некоторые важные элементы для завершения SSL VPN конфигурации,
опущены. Для SSL-VPN, все FortiGates должны использовать тот же порт TCP.
Включение VPN автосоединения
VPN Auto Connect использует следующие XML тег:
<autoconnect_tunnel> ipsecdemo.fortinet.com </ autoconnect_tunnel>
Внутри:
<vpn>
<options>
Запомнить пароль также необходимо, потому что это автосоединения:
<save password>1 </ save password>
Включение VPN всегда VPN всегда используются следующие XML тег:
<keep_running> 1 </ keep_running>
Внутри:
<vpn>
<connection>
Расширенные функции (Mac OS X)
Создания избыточного IPsec VPN
Для использования VPN отказоустойчивости / резервирования, вы будете настроить
список серверов FortiGate IP / FQDN, вместо одного:
<forticlient_configuration>
<vpn>
<ipsecvpn>
<options>
...
</ Функции>
<connections>
<connection>
<name> psk_90_1 </ Name>
<type> руководства </ Туре>
<ike_settings>
<prompt certificate> 0 </ prompt certificate>
<server> 10.10.90.1; ipsecdemo.fortinet.com; 172.17.61
0.143 < cepbep>
<redundantsortmethod> 1 </ redundantsortmethod>
...
</ Ike settings>
</ Связь>
</ Подключения>
</ Ipsecvpn>
</ VPN>
</ Forticlient configuration>
Это сбалансированная, но неполное XML фрагмент конфигурации. Все закрывающие теги
включены, но некоторые важные элементы для завершения конфигурации IPsec VPN,
опушены.
RedundantSortMethod = 1
Этот тег XML устанавливает соединение IPsec VPN, как пинг-ответ, основанный. VPN
будут подключаться к FortiGate который отвечает самым быстрым.
RedundantSortMethod = 0
По умолчанию RedundantSortMethod = 0, и соединение IPsec VPN является приоритет,
основанный. Приоритет конфигурации на основе будет пытаться подключиться к
```

FortiGate начиная с первой в списке. Приоритет, основанный SSL-VPN соединений SSL-VPN поддерживает конфигурации на основе приоритета для избыточности. <forticlient\_configuration> <vpn> <sslvpn> <options> <enabled> 1 </ включен> ... </ Функции> <connections> <connection> <name> ssl 90 1 </ Name> <server> 10.10.90.1; ssldemo.fortinet.com; 172.17.61.143:44 3 </ сервер> ... </ Связь> </Подключения> </ SSLVPN> </ VPN> </ Forticlient configuration> Это сбалансированная, но неполное XML фрагмент конфигурации. Все закрывающие теги включены, но некоторые важные элементы для завершения SSL VPN конфигурации, опущены. Для SSL-VPN, все FortiGates должны использовать тот же порт TCP. Включение VPN автосоединения VPN Auto Connect использует следующие XML тег: <autoconnect tunnel> SSL 198 не CERT </ autoconnect tunnel> Включение VPN всегда VPN всегда используются следующие XML тег: <keep\_running> 1 </ keep\_running> VPN туннеля и сценарий (Windows) Обзор функций Эта функция поддерживает автоматический запуск пользовательского сценария после настроено VPN туннель подключены или отключены. Сценарии пакетных сценариев в окнах и скрипты в Мас OS X. Они будут определены как часть конфигурации VPN туннелей на XML формат FortiGate автора Endpoint профиля. Профиль будет толкнул вниз, чтобы FortiClient от FortiGate. Когда VPN туннеля FortiClient в подключении или отключении, соответствующие сценарию, что определено в Туннель будет выполнен. VPN перед входом в настоящее время не поддерживается в FortiClient v5.0 Патч Release 1 (Mac OS X). Подключить сетевой диск после туннельное соединение Сценарий будет подключить сетевой диск и скопировать некоторые файлы после туннеля связано. <on connect> <script> <OS> окна </ OS> <script> <script> <! [CDATA [ NET USE X: \\ 192.168.10.3 \ ftpshare / пользователь: Мед Бу-Бу

MD C: \ Test Копия X:  $\ PDF \ * * C:. \ Test$ ]]> </ SCRIPT> </ SCRIPT> </ SCRIPT> </ On\_connect> Удаление сетевого диска после туннеля отключен Сценарий будет удалить сетевой диск после туннеля отключен. <on disconnect> <script> <OS> окна </ OS> <script> <script> <! [CDATA [ Чистая x использования: / DELETE ]]> </ SCRIPT> </ SCRIPT> </ SCRIPT> </ On disconnect> VPN туннеля и сценарий (Mac OS X) Подключить сетевой диск после туннельное соединение Сценарий будет подключить сетевой диск и скопировать некоторые файлы после туннеля связано. <on\_connect> <script> <OS> Mac </ OS> <script> / BIN / MkDir / Volumes / инсталляторов / Sbin / пинг-С 4 192.168.1.147> / Users / Admin / Desktop / Dropbox / p.txt / Sbin / Mount-T SMBFS // Kimberly: RigUpTown@ssldemo.fortinet.com / установки Fortinet Технологии Инк Страница 58 FortiClient v5.0 Руководство администратора S / Volumes / строителей /> / Users / Admin / Desktop / Dropbox / m.txt / BIN / MkDir / Users / Admin / Desktop / Dropbox / каталог / BIN / CP / Volumes / строителей / \*. Журнал / Users / Admin / Desktop / Dropbox / каталог /. </ SCRIPT> </ SCRIPT> </ On\_connect> Удаление сетевого диска после туннеля отключен Сценарий будет удалить сетевой диск после туннеля отключен. <on disconnect> <script> <OS> Mac </ OS> <script> / Sbin / размонтирование / Volumes / инсталляторов

/ BIN / RM-FR / Users / Admin / Desktop / Dropbox / \*

</ SCRIPT>

</ SCRIPT>

</ On\_disconnect>

Для получения дополнительной информации см. FortiClient v5.0 Справочник по XML в Fortinet Технические Документация сайт, http://docs.fortinet.com.

Страница 59

Поиски уязвимости

FortiClient v5.0 включает в себя модуль поиска уязвимостей и проверить персональный компьютер для известные уязвимости системы.

В этом разделе описывается, как включить поиск уязвимостей, и параметры конфигурации.

Scan Now

Для выполнения поиска уязвимостей, выберите кнопку Scan Now на FortiClient приборной панели.

FortiClient будет сканировать ваш персональный компьютер на наличие известных уязвимостей. Приборная панель отмечает дату последнего сканирования выше кнопки. Рисунок 61: Поиск уязвимостей в прогрессе.



# Обновить сейчас

Выберите кнопку Обновить на панели FortiClient для обновления. Когда проверка завершится, FortiClient будет отображать количество уязвимостей, обнаруженных на приборной панели. Выберите найдена ссылка на просмотр списка уязвимостей, обнаруженных в вашей системе.

Рисунок 62: Уязвимости, обнаруженные страницы.

Vulnerabilities Detected in the Last 30 Days					
Vulnerability Name	Severity	Details	Time		
Most Recent Scan					
1 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-24	Critical	33877	24/12/2012 2:35:21 PM		
2 MS.VS.Active.Template.Library.Remote.Code.Execution	Critical	20531	24/12/2012 2:35:21 PM		
3 Oracle.Java.SE.Critical.Patch.Update.October.2012	Critical	33716	24/12/2012 2:35:21 PM		
4 Oracle.Java.SE.Critical.Patch.Update.Advisory.February.2012	Critical	32669	24/12/2012 2:35:21 PM		
5 Oracle.Java.SE.Critical.Patch.Update.February.2011	Critical	27928	24/12/2012 2:35:21 PM		
6 Oracle.Java.SE.Critical.Patch.Update.June.2011	Critical	30899	24/12/2012 2:35:21 PM		
7 Oracle.Java.Runtime.True.Type.Font.IDEF.Opcode.Buffer.Ove	Critical	31444	24/12/2012 2:35:21 PM		
8 Oracle.Java.Runtime.Environment.Memory.Corruption.Vulnera	Critical	33599	24/12/2012 2:35:21 PM		
9 Oracle.Java.MixerSequence.Array.Index.Remote.Code.Execut	Critical	30551	24/12/2012 2:35:21 PM		
10 Oracle.Java.FileDialog.Show.Buffer.Overflow	Critical	28761	24/12/2012 2:35:21 PM		
11 Oracle.Java.SE.Critical.Patch.Update.June.2012	Critical	32430	24/12/2012 2:35:21 PM		
12 Microsoft.XML.Core.Services.Remote.Code.Execution.Vulner	Critical	32958	24/12/2012 2:35:21 PM		
13 MS.Windows.Unauthorized.Digital.Certificates.Spoofing.KB2	Critical	32685	24/12/2012 2:35:21 PM		
14 Apple.Safari.Multiple.Vulnerabilities.APPLE-SA-2012-11-01-2	Critical	33927	24/12/2012 2:35:21 PM		
15 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-14	Critical	32255	24/12/2012 2:35:21 PM		
16 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-19	Critical	33028	24/12/2012 2:35:21 PM		
17 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-22	Critical	33582	24/12/2012 2:35:21 PM		
Close	Clear				

Выберите номер Details ID из списка, чтобы просмотреть информацию о выбранном уязвимость FortiGuard сайта. На сайте подробно дате выпуска, степень тяжести,, описание, пострадавшим продуктов, и рекомендуемые действия.

Уязвимость Имя уязвимости

Суровость. Степень серьезности назначен на уязвимости, критические, высокий, средний, Низкий, информация.

Детали. FortiClient поиска уязвимостей перечисляет Bugtraq (BID) номер, под подробнее колонки. Вы можете выбрать BID для просмотра сведений о уязвимости FortiGuard на сайте, или искать в Интернете с помощью этой ставки числа. Время. Дата и время, что уязвимость была обнаружена.

Близко. Закрыть окно и вернуться к FortiClient приборной панели.

Очистить. Очистить результаты поиска уязвимостей.

Рисунок 63: Подробности FortiGuard сайте.

	🏦 🏙 Library. 🤍 Tools Q
Oracle. Java. SE. Critical. Patch. Update. June. 2012 Release Date	
Jun 29, 2012 Severity critical	
Impact The exploitation of these vulnerabilities could result in arbitrary code execution or lead to denial of service.	

Поиск уязвимостей регистрации.

Для настройки ведения журнала поиска уязвимостей, выберите Файл на панели инструментов, и настройки на раскрывающемся меню. Выберите вход, чтобы посмотреть в выпадающем меню. Выберите поиск уязвимостей на вход меню позволяет включить ведение журнала для этого модуля.

# Резервного копирования или восстановления полной конфигурации

Для резервного копирования или восстановления полного файла конфигурации Файл выберите на панели инструментов и настройки на раскрывающемся меню. Выберите Система, чтобы посмотреть в выпадающем меню. В этом меню вы можете выполнить резервного копирования или восстановления файла конфигурации.

Рисунок 64: Резервное копирование и восстановления данных.

System		
Backup or restore full configuration	Backup	Restore
Software update: <a>Automatically down</a>	nload and install up	dates
O Alert when updates	s are available	

При выполнении резервного копирования можно выбрать конечный файл и сохранить файл в незашифрованном или зашифрованном виде.

Рисунок 65: Параметры резервного копир File Help	ования файлов.	
▼ System		
Backup or restore full configuration	Backup	Restore
Software update: (     Automatically dow	nload and install up	dates
Alert when update	s are available	

Select Destination		
Password		
Confirm		
No I	Password	
OK	Connel	
UK	Cancer	

Чтобы настроить ведение журнала, выберите Файл на панели инструментов и настройки на выпадающее меню. Вход для просмотра выпадающего меню. В этом меню вы можете настроить ведение журнала для следующих

Особенности: VPN Антивирус Обновление

#### Application Firewall

Родительский контроль

Поиск уязвимостей.

Вы можете задать уровень ведения журнала и выберите для экспорта бревен или Очистить журналы.

Рисунок 66: Вход варианты.

#### Logging

Enable logging fo	r these features:	VPN	V Application Firewall
		🗸 AntiVirus	Parental Control
		V Update	Vulnerability Scan
Log Level	Information 💌		
Log file	Export logs Clear log	<u>s</u>	

#### Обновления

Для настройки обновлений, выберите Файл на панели инструментов и настройки на выпадающее меню. Выбрать в системе, чтобы посмотреть в раскрывающемся меню. В этом меню вы можете настроить поведение FortiClient, когда новая версия программного обеспечения доступна на серверах FortiGuard Распределение (FDS). Уровень регистрации

Описание

Аварийный

Система становится неустойчивой.

Оповещение

Требуются незамедлительные действия.

Критический

Функциональность влияет.

Ошибка

Ошибка существует и функциональность может быть затронуто.

Предупреждение

Функциональность может быть затронуто.

Замечать

Информация о нормальных событий.

Информация

Общая информация о системе операций.

Отлаживать

Отладка FortiClient.

Рисунок 67: Обновление варианты.

•	System	

Backup or restore	full configuration	Backup	Restore
Software update:	Automatically down	ates	
	O Alert when updates	are available	

#### VPN варианты

Для настройки VPN параметров выберите Файл на панели инструментов и настройки на выпадающее меню. Выберите VPN функции для просмотра выпадающего меню. В этом меню вы можете настроить для предоставления VPN перед входом в систему. Рисунок 68: VPN варианты.



Enable VPN before logon

#### Управление сертификатами

Для настройки VPN сертификатов, выберите Файл на панели инструментов и настройки на выпадающее меню. Выбор сертификата, чтобы просматривать выпадающего меню. В этом меню вы можете настроить IPsec VPN использовать локальные сертификаты и сертификаты для импорта FortiClient.

Рисунок 69: Параметры сертификата.

Certificate Management

Use local certificate uploads (IPSec only)

Certificate	Туре	Valid To	Action
			Import

# Параметры антивируса

Чтобы настроить параметры антивируса, выберите Файл на панели инструментов, и настройки на выпадающее меню. В этом меню вы можете настроить нежелательные варианты и поведение FortiClient при обнаружении вируса.

Рисунок 70: параметры антивируса.

AntiVirus Options

Grayware Options

🔽 Adware 📝 Riskware

Alert when viruses are detected

Pause background scanning on battery power

Enable FortiGuard Analytics

#### Дополнительные параметры

Чтобы настроить дополнительные параметры, выберите Файл на панели инструментов, и настройки на выпадающее меню.

Выберите Дополнительно, чтобы посмотреть в выпадающем меню. В этом меню вы можете настроить WAN.

Оптимизация, единого входа, настройки синхронизации с FortiGate, отключите прокси, а по умолчанию FortiClient вкладку при запуске.

Рисунок 71: Усовершенствованные функции.

Advanced		
V Enable WAN Optimizat	tion	
Maximum Disk Cac	he Size:	512 MB
V Enable Single Sign-On	n mobility agent	
Server address		
Customize port	8001	
Pre-Shared Key		
Disable configuration :	sync with FortiGate	
📝 Disable proxy (trouble	eshooting only)	
Default tab AntiVirus	•	

#### Опции нежелательных программ

Нежелательных программ это зонтичный термин применяется к широкому кругу Вредоносные программы, такие как шпионское, рекламное ПО, которые часто тайно установленных на компьютере пользователя, чтобы отслеживать и сообщать определенную информацию на внешние источники без разрешения пользователя. Выберите, чтобы включить обнаружение сканирование в реальном времени.

#### Потенциально опасные программы

Выберите, чтобы включить обнаружение потенциально опасных программ и карантина в течение антивирусное сканирование.

#### Сигнал тревога когда вирусы обнаруженный

Выберите для отображения окна уведомление когда вирус обнаружено.

#### Пауза фоне сканирования от батареи

Выберите, чтобы приостановить фоновое сканирование при питании от аккумулятора. Включить FortiGuard Analytics Выберите для автоматической отправки подозрительных файлов в FortiGuard.

#### Сеть для анализа.

#### Single Sign-On агента мобильности

FortiClient Single Sign-On Мобильность агент выступает в качестве клиента, который с обновлениями FortiAuthenticator с входа пользователя в систему и информационную сеть. FortiAuthenticator прослушивает конфигурируемых порта TCP. FortiClient подключается к FortiAuthenticator использованием TLS / SSL с двусторонней проверки подлинности сертификата. FortiClient посылает вход в систему пакет FortiAuthenticator, которая отвечает с пакет подтверждения.

FortiClient / FortiAuthenticator связи требуется следующее:

IP-адрес должен быть уникальным в пределах всей сети.

FortiAuthenticator должна быть доступна с клиентами во всех регионах.

FortiAuthenticator должны быть доступны для всех FortiGates.

Включить Single Sign-On агента мобильности на FortiClient

1. Выберите файл на панели инструментов и настройки на выпадающее меню.

2. Выберите Дополнительно, чтобы посмотреть в выпадающем меню.

3. Выберите, чтобы включить Single Sign-On агента мобильности.

Включить WAN Оптимизация

Выберите, чтобы включить оптимизации глобальной сети. Вы должны включить, только если вы FortiGate сконфигурирован для WAN

Оптимизация.

Максимальная лиска Размер кэш-памяти Выберите, чтобы настроить максимальный размер дискового кэша. Значение по vмолчанию 512 Mб. Включить Single Sign-On агента мобильности Выберите, чтобы включить Single Sign-On Arent для мобильных FortiAuthenticator. Для использования этой функции необходимо применить FortiClient SSO мобильности лицензии areнта FortiAuthenticator вашего устройства. Адрес сервера Введите адрес FortiAuthenticator IP. Настроить порт Введите номер порта. По умолчанию используется порт 8001. Pre-Shared Key Введите общий ключ. Предварительный ключ должен совпадать с ключом настроенный на FortiAuthenticator. Отключить конфигурацию синхронизации с FortiGate Выберите, чтобы отключить синхронизацию с конфигурацией FortiGate. Отключить прокси (Диагностика только) Выберите, чтобы отключить прокси при устранении FortiClient. Закладку по умолчанию Выберите закладку по умолчанию, который будет отображаться при открытии FortiClient. FortiClient Single Sign-On агента мобильности требует FortiAuthenticator работает v2.0.0 **GA** сборки 0006 или более поздней версии. Введите FortiAuthenticator (сервер) IP-адрес, номер порта, и с предварительным общим настроен ключ на FortiAuthenticator.

Fortinet Технологии Инк

4. Введите адрес FortiAuthenticator сервера и предварительный ключ.

Включить FortiClient SSO Мобильность Агент службы по FortiAuthenticator

1. Выберите SSO и динамической политики> SSO> Параметры.

2. Выберите Включить FortiClient SSO Мобильность Service Agent и значение TCP порт для прослушивания

порт.

3. Выберите Включить аутентификацию и ввести секретный ключ значение.

Рисунок 72: Конфигурация FortiAuthenticator.

FortiAuthenticat	tor		Logged in as <b>admin</b>	Help Logout	FERTIDET
System		Edit	FSSO Configuration		
Authentication	FortiGate				
SSO & Dynamic Policies	Listening port:	8000			
SSO SSO	Login expiry (minutes):	480			
	Enable authentication				
- SSO Groups	Secret key:	•••••			
<ul> <li>– • Domain Controllers</li> <li>– • Radius Accounting</li> </ul>	Log level:	Info _			
FortiGate Group Filtering	Fortinet Single Sign-On (i	-SSO)			
Dynamic Policy	Enable Windows Active D	irectory domain controllers			
Accounting Proxy	Enable Radius Accounting	3 SSO clients			
- • Rule Sets	Use remote LDAP serv	er for SSO groups lookup			
Destinations	LDAP server:	[Please Select]			
	Enable FortiClient SSO M	obility Agent Service			
	Listening port.	8001			
	☑ Enable authentication				
Monitor	Secret key:	•••••			
Certificate Management			OF		
Logging			UK		

4. Чтобы включить FortiClient FSSO услуг на интерфейсе выберите Система > Сеть > интерфейс.

Выберите Изменить для изменения сетевого интерфейса, выберите FortiClient FSSO включить.

Рисунок 73: Включение служб.

FortiAuthenticator	1			Logged in as a	admin 🕜 Help	Logout	F
System			Edit	Network Interface			
Dashboard Inte	erface Status						
Status Inter	rface:	port1					
Network Stat	us:	0					
DNS	Address / Ne	tmask					
Static Routing	ł:	172.16.68.48/255.255.255.0					
i ∰ Maintenance IPv6 IPv6	ð:						
Acc	ess Rights						
Adm	nin access:	☑ Telnet ☑ SSH ☑ HTTPS ☑ HTTP					
Serv	vices:	<ul> <li>☑ RADIUS Auth</li> <li>☑ RADIUS Accounting</li> <li>☑ LDAP</li> </ul>					
Authentication		☑ LDAPS					
SSO & Dynamic Policies		✓ FortiGate FSSO ✓ OCSP					
Monitor		FortiClient FSSO					
Certificate Management							
Logging	ory		ОК	Cancel			

Чтобы включить SSO Мобильность FortiClient Агент службы по FortiAuthenticator, вы должны сначала применяется соответствующая лицензия FortiClient для FortiAuthenticator. Для получения дополнительной информации см. FortiAuthenticator v2.0 Руководство администратора на http://docs.fortinet.com. Для получения информации о приобретение лицензии на FortiClient FortiAuthenticator, пожалуйста, обратитесь к своему уполномоченному Fortinet реселлера.

# Конфигурация блокировки

Для предотвращения несанкционированных изменений в FortiClient конфигурации, выберите значок замка расположены в левом нижнем углу страницы настройки. Вам будет предложено ввести и подтвердить пароль.

Когда конфигурация заблокирована, изменения конфигурации ограничен и не может FortiClient быть закрыты или удалены.

Рисунок 74: Настройка блокировки.

Please Provide Password			22
Password			
Confirm			
▼ R(	OK Cance		
Specify FortiGate addres	s		
✓ Default gateway			
✓ Listen for broadcast mes.	sades		
▼ VPN Options			
Click the lock to protect confi	uration changes	ОК	Cancel
	juration changes		
Посмотреть нарушений Application Firewall Посмотреть Блокировка прилож Удаленный доступ Настройка, изменение и удалени Подключение к VPN-соединени Поиск уязвимостей Выполните поиск уязвимостей о Посмотреть уязвимостей	сений ие IPsec VPN или SSL V ия системы	/PN-соединения	I
Регистрации и отмены регистра	ции FortiClient для конт	гроля конечных	точек
Настройки			
Экспорт FortiClient журналы	manuu FortiCliant		
Лля выполнения изменений кон	ирации гописпені Прации или закрыті	ь FortiClient вы	берите значок замка
и введите Пароль, используемы	й для блокировки конф	игурации.	septite shu tok sumk
FortiTray		51	
Когда FortiClient работает на вал системный трей для выполнения	шей системе, вы может я различных действий.	е выбрать Fortil Значок FortiTray	гау значок на окнах у доступен в
системном трее даже, когда пан	ель FortiClient закрыт.		
Открытое FortiClient консоли	ию		
Shutdown FortiClient			
Линамические параметры меню	в зависимости от конd	оигурации	

Динамические параметры меню в зависимости от конфигураци Подключение к настроено IPsec VPN или SSL VPN-соединени

Откройте окно антивирусной проверки (если проверка по расписанию в данный момент)

Откройте окно поиска уязвимостей (если поиск уязвимостей работает)

При наведении курсора мыши на значок FortiTray, вы будете получать различные уведомления включая версию, А.В. подпись, А. В. двигателя.

Рисунок 75: Значок в системной панели.



Когда конфигурация заблокирована, опция для закрытия FortiClient от FortiTray неактивна вне.

### Подключение к VPN-соединения

Для подключения к VPN-соединения от FortiTray выберите задач Windows и щелкните правой кнопкой на иконку FortiTray. Выберите соединение, которое вы хотите подключиться, введите имя пользователя и пароль в окно аутентификации и выберите ОК для подключения.

Рисунок 76: Окно аутентификации.

Authentication Information			
Username	tmosby@fortinet.com		
Password	•••••		
	📝 Remember Username		
	ОК	Cancel	

http://www.fortinet.com