**ПРОФЕСИОНАЛНА ГИМНАЗИЯ**

**ПО**

**БИТОВА ТЕХИНКА**

**ПЛОВДИВ**

**РЕФЕРАТ**

по **КОМЮТЪРНИ МРЕЖИ**

на тема:

**5-ТЕ НАЙ-РАЗПРОСТРАНЕНИ СОФТУЕРНИ ЗАЩИТНИ СТЕНИ**

**Изготвил:** Павлин Попов **Проверил:** Инж. Пенка Янева

*2023*

**УВОД**

Защитна стена е система за мрежова сигурност, която наблюдава и контролира входящия и изходящия мрежов трафик въз основа на предварително определени правила и политики за сигурност. Защитните стени могат да бъдат базирани на хардуер или софтуер и се използват за защита на мрежа от неоторизиран достъп, злонамерен софтуер и други кибер заплахи. Те могат да се използват и за контрол на достъпа до специфични мрежови ресурси или за ограничаване на достъпа до интернет. Защитните стени са важен компонент от цялостната стратегия за сигурност за всяка организация.

Първата защитна стена е създадена в края на 80-те години на миналия век от основателя на Digital Equipment Corporation, Уилям Чезуик и Стивън Беловин, и двамата изследователи в AT&T Bell Labs. Името "защитна стена" произлиза от концепцията за физическа защитна стена в сграда, която се използва за предотвратяване на разпространението на пожар.

Защитните стени могат да се използват за блокиране на определени типове трафик, като споделяне на файлове между партньори, за да попречат на служителите да губят вниманието си за дейности, които не са свързани с работата. Те могат също да се използват за блокиране на достъпа до конкретни уебсайтове, като сайтове за социални медии. Защитните стени могат да бъдат конфигурирани да позволяват отдалечен достъп до мрежа, като например чрез VPN, за да могат служителите да работят от вкъщи или други отдалечени места.

Най-вече се използват за наблюдение на мрежовия трафик за подозрителна дейност и да предупреждават мрежовите администратори за потенциални пробиви в сигурността. Те могат също да се използват за блокиране на входящ трафик от определени държави, за предотвратяване на атаки от известни злонамерени източници.

Политиките на защитната стена могат да бъдат сложни и може да изискват работата на мрежови администратори и експерти по сигурността за настройка и поддръжка. Някои устройства със защитна стена могат да бъдат конфигурирани да работят заедно с други инструменти за сигурност, като системи за откриване и предотвратяване на проникване (IDPS) или системи за управление на информация и събития за сигурност (SIEM), за да осигурят по-всеобхватно решение за сигурност.

Важно е софтуерът и фърмуерът на защитната стена да се актуализират, за да се гарантира, че са налице най-новите корекции и функции за сигурност, тъй като защитната стена често се счита за първата линия на защита в стратегията за мрежова сигурност, но не е достатъчно да разчитате само на защитната стена, тъй като тя не може да защити срещу всички форми на кибератаки.

Важно е да се гарантира, че защитната стена може да обработва криптиран трафик. С нарастващото използване на криптиране за защита на чувствителни данни, защитните стени трябва да могат да проверяват и контролират криптирания трафик, без да оказват отрицателно въздействие върху производителността.

**Видове защитни стени**

Има няколко вида защитни стени, включително мрежови защитни стени, хост-базирани защитни стени, защитни стени за проверка на състоянието, защитни стени на ниво приложение, защитни стени от следващо поколение, базирани на облак защитни стени, безжични защитни стени, защитни стени за Unified Threat Management (UTM), софтуерно дефинирани защитни стени и хардуерно базирани защитни стени. Изборът на тип защитна стена ще зависи от специфичните нужди и изисквания на организацията.

Някои от най-често срещаните типове защитни стени включват:

1. Мрежови защитни стени: Това са най-често срещаният тип защитни стени и обикновено се внедряват в периметъра на мрежата. Те се използват за контролиране на достъпа до мрежа чрез филтриране на входящия и изходящия трафик въз основа на предварително определени правила за сигурност.
2. Хост-базирани защитни стени: Те са инсталирани са на отделни хост компютри и се използват за защита на един хост от мрежови атаки. Те обикновено се използват в допълнение към мрежовите защитни стени за допълнителна сигурност.
3. Държавни стени за проверка на състоянието: Тези защитни стени следят състоянието на мрежовите връзки и са в състояние да вземат по-информирани решения за това дали да разрешат или блокират трафика.
4. Защитни стени на ниво приложение: Целта на тези стени е да проверяват и контролират трафика на ниво приложение, а не на ниво мрежа. Те са в състояние да идентифицират и контролират конкретни протоколи за приложения, като HTTP или FTP, и могат да се използват за контрол на достъпа до конкретни приложения.
5. Защитни стени от следващо поколение: Тези защитни стени са по-нов тип защитни стени, които съчетават характеристиките на традиционните защитни стени с по-нови технологии за сигурност, като предотвратяване на проникване, контрол на приложения и пясъчна среда.
6. Облачна защитна стена: Те се управляват и хостват от доставчик на облачни услуги и се използват за защита на базирани на облак приложения и данни от кибератаки.
7. Безжична защитна стена: Използват се за защита на безжичните мрежи от неоторизиран достъп и други специфични за безжичната мрежа заплахи.
8. Защитни стени за Unified Threat Management (UTM): Тези защитни стени предлагат цялостно решение за сигурност, което включва функции като защитна стена, предотвратяване на проникване, антивирусна програма и филтриране на съдържание в едно устройство.
9. Софтуерно дефинирани защитни стени: Внедрени в софтуер, обикновено като виртуална машина. Те са гъвкави, лесни за внедряване и могат да се управляват дистанционно.
10. Хардуерни защитни стени: Те се внедряват с помощта на специални хардуерни устройства, като рутери или уреди. Те обикновено са по-скъпи от софтуерно базираните защитни стени, но могат да осигурят по-висока производителност и по-разширени функции.

Изборът на тип защитна стена ще зависи от специфичните нужди и изисквания на организацията. В някои случаи може да се използва комбинация от различни видове защитни стени за допълнителна сигурност.

**Съвместимост**

Когато става въпрос за съвместимост на защитната стена в сървъри или клиенти, важно е да се гарантира, че защитната стена е съвместима с операционната система и друг софтуер, работещ на сървъра или клиента. Някои защитни стени са проектирани специално за определени операционни системи, като Windows или Linux, и може да не са съвместими с други операционни системи. Освен това е важно да се гарантира, че защитната стена пасва с всеки друг софтуер или приложения, работещи на сървъра или клиента. Например, ако сървърът или клиентът изпълнява конкретен уеб сървър или софтуер за база данни, защитната стена трябва да може да обработва трафика, генериран от този софтуер, и да разрешава или блокира достъпа, ако е необходимо. Трябва да се провери дали защитната стена е съвместима с всички други мерки за сигурност, като системи за откриване и предотвратяване на проникване, антивирусен софтуер. Защитната стена трябва да може да се интегрира с други мерки за сигурност, като IPS и IDS, за да осигури по-цялостно решение за сигурност. Друг важен аспект на съвместимостта на защитната стена в сървъри или клиенти е способността да се поддържат различни протоколи, като TCP/IP, UDP и ICMP. Защитните стени трябва да могат да проверяват и контролират трафика за тези протоколи, както и за всички други протоколи, които се използват в мрежата. Това ще гарантира, че целият трафик се наблюдава правилно и контролира от защитната стена, осигурявайки по-добра сигурност.

Съвместимостта на защитната стена в сървъри или клиенти е важно съображение при избора и внедряването и. Важно е да се гарантира, че защитната стена е съвместима с операционната система и друг софтуер, работещ на сървъра или клиента, както и всички други мерки за сигурност, за да се осигури цялостно и ефективно решение за защита. Когато инсталирате защитна стена, е важно да проверите уебсайта на доставчика, за да се уверите дали има известни проблеми с операционната система. Важно е да се гарантира, че защитната стена може да се справи с обема на трафика и изискванията за производителност на мрежата. Например, ако се очаква сървърът или клиентът да обработва голямо количество трафик, защитната стена трябва да разполага с необходимия хардуер и софтуер, за да обработва този трафик, без да причинява проблеми с производителността. Също така трябва да се провери мащабируемостта на защитната стена, тя трябва да може да се справи с нарастването на мрежата и променящите се изисквания за сигурност. Това ще гарантира, че защитната стена може да продължи да осигурява ефективна сигурност, докато мрежата расте и се развива. Защитната стена може да бъде интегрирана с други инструменти и системи за сигурност като SIEM, управление на идентичността и достъпа и платформи за оркестрация, автоматизация и реакция на сигурността (SOAR). Това ще осигури по-всеобхватно решение за сигурност чрез интегриране на различни инструменти и системи за сигурност, които да работят заедно за откриване, предотвратяване и реагиране на заплахи за сигурността.

И накрая, важно е да се гарантира, че защитната стена може лесно да се управлява и конфигурира. Защитните стени трябва да имат удобен за потребителя интерфейс и трябва да бъдат лесни за конфигуриране и управление от разстояние. Това ще улесни мрежовите администратори да актуализират и поддържат своите политики за защитна стена и ще гарантира, че защитната стена винаги осигурява ефективна защита. Технологията на защитната стена непрекъснато се развива, като през цялото време се добавят нови функции и възможности, като предотвратяване на проникване, контрол на приложения и пясъчна среда.

**Виртуализация**

Друго важно съображение, когато става дума за съвместимост на защитната стена в сървъри или клиенти, е способността да се поддържат технологии за виртуализация като VMWare, Hyper-V и Virtual Box. Много организации се насочват към виртуализация като начин за намаляване на разходите и подобряване на ефективността. Защитните стени трябва да могат да защитават виртуализирани среди по същия начин, както физическите среди. Някои доставчици на защитни стени предлагат специализирани решения за защитни стени за виртуализирани среди, които включват функции като интроспекция на виртуална машина и микросегментиране, за да осигурят по-добра сигурност в тези среди.

**Мобилни устройства**

Добра възможност на продукта е да поддържа мобилни устройства като лаптопи, смартфони и таблети. Защитните стени трябва да могат да наблюдават и контролират трафика от тези устройства, независимо дали са свързани към мрежата чрез кабелна или безжична връзка. Това ще гарантира, че целият трафик от мобилни устройства се наблюдава правилно и контролира от защитната стена, осигурявайки по-добра сигурност.

**Платени/Безплатни**

Платените защитни стени обикновено се разработват и продават от търговски компании и предлагат широка гама от функции и възможности, като разширена защита от заплахи, предотвратяване на проникване и контрол на приложения. Те често се считат за по-надеждни, сигурни и имат по-разширени функции от безплатните, но могат да бъдат по-скъпи. Платените защитни стени обикновено се използват от организации с големи мрежи, като корпорации и правителствени агенции, които изискват високо ниво на сигурност и имат ресурсите да инвестират в усъвършенствани решения за защитни стени.

Безплатните защитни стени, от друга страна, обикновено са решения с отворен код или безплатни софтуерни решения, които са достъпни за изтегляне в интернет. Те могат да бъдат добър вариант за малки фирми или домашни потребители, които търсят основно ниво на сигурност и не искат да инвестират в платено решение за защитна стена. Безплатните защитни стени може да нямат толкова много функции, колкото платените, но все пак могат да осигурят основно ниво на сигурност. Освен това някои безплатни защитни стени са с отворен код, което означава, че общността може да помогне за подобряването и поддържането им.

Важно е да се отбележи, че макар безплатните защитни стени да са по-евтини от платените, те може да не предоставят същото ниво на сигурност, нито същото ниво на поддръжка. Освен това безплатните защитни стени може да нямат същото ниво на мащабируемост като платените защитни стени, което означава, че може да не са в състояние да се справят с обема на трафика и изискванията за производителност на голяма мрежа.

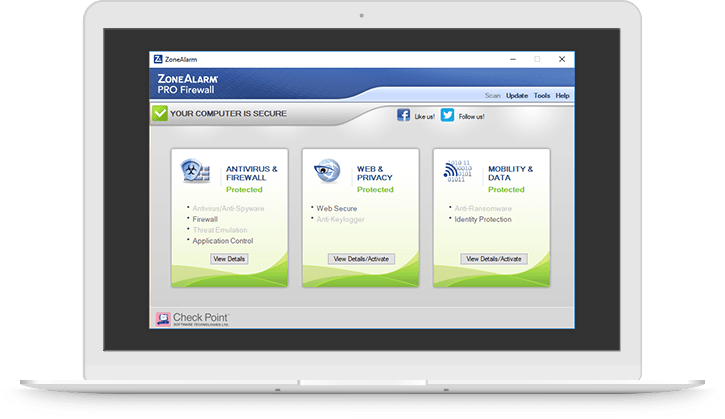
Както платените, така и безплатните защитни стени имат своите предимства и недостатъци. Платените защитни стени обикновено са по-модерни и надеждни, но могат да бъдат и по-скъпи. Безплатните защитни стени могат да бъдат добър вариант за малки фирми или домашни потребители, които търсят основно ниво на сигурност и не искат да инвестират в платено решение за защитна стена, но може да не предоставят същото ниво на сигурност, нито същото ниво на платени защитни стени.

**ZoneAlarm**. Това е програма антивирусна и защитна стена в едно. Базирана е да се използва само в Windows среда. Тя защитава компютъра от неоторизиран достъп и контролира потока на входящия и изходящия мрежов трафик. Работи, като наблюдава и контролира мрежовите връзки на компютър и блокира всеки подозрителен или нежелан трафик. ZoneAlarm предлага разнообразие от функции, които помагат за защита на компютъра от различни видове мрежови заплахи, включително зловреден софтуер, хакерски атаки и опити за фишинг. Някои от функциите включват:

* Двупосочна защитна стена, която следи както входящия, така и изходящия трафик.
* Разширена защита при изтегляне, която сканира файловете за злонамерен софтуер, преди да бъдат изтеглени.
* Защита на самоличността, която предупреждава потребителите за потенциални опити за кражба на самоличност.
* Автоматични актуализации, за да се гарантира, че програмата е винаги актуална.

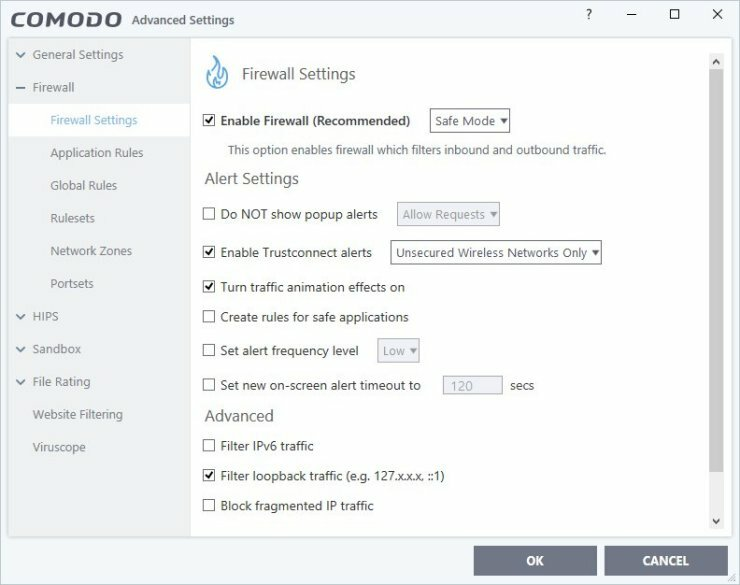
ZoneAlarm предлага както платена, така и безплатна версия. Безплатната версия осигурява основна защита на системата, докато платената версия предлага допълнителни функции като разширена защита при изтегляне и защита на самоличността. Няма демо версия на програмата, но има безплатна пробна версия на платената версия, която можете да използвате, за да изпробвате допълнителните функции, преди да купите.

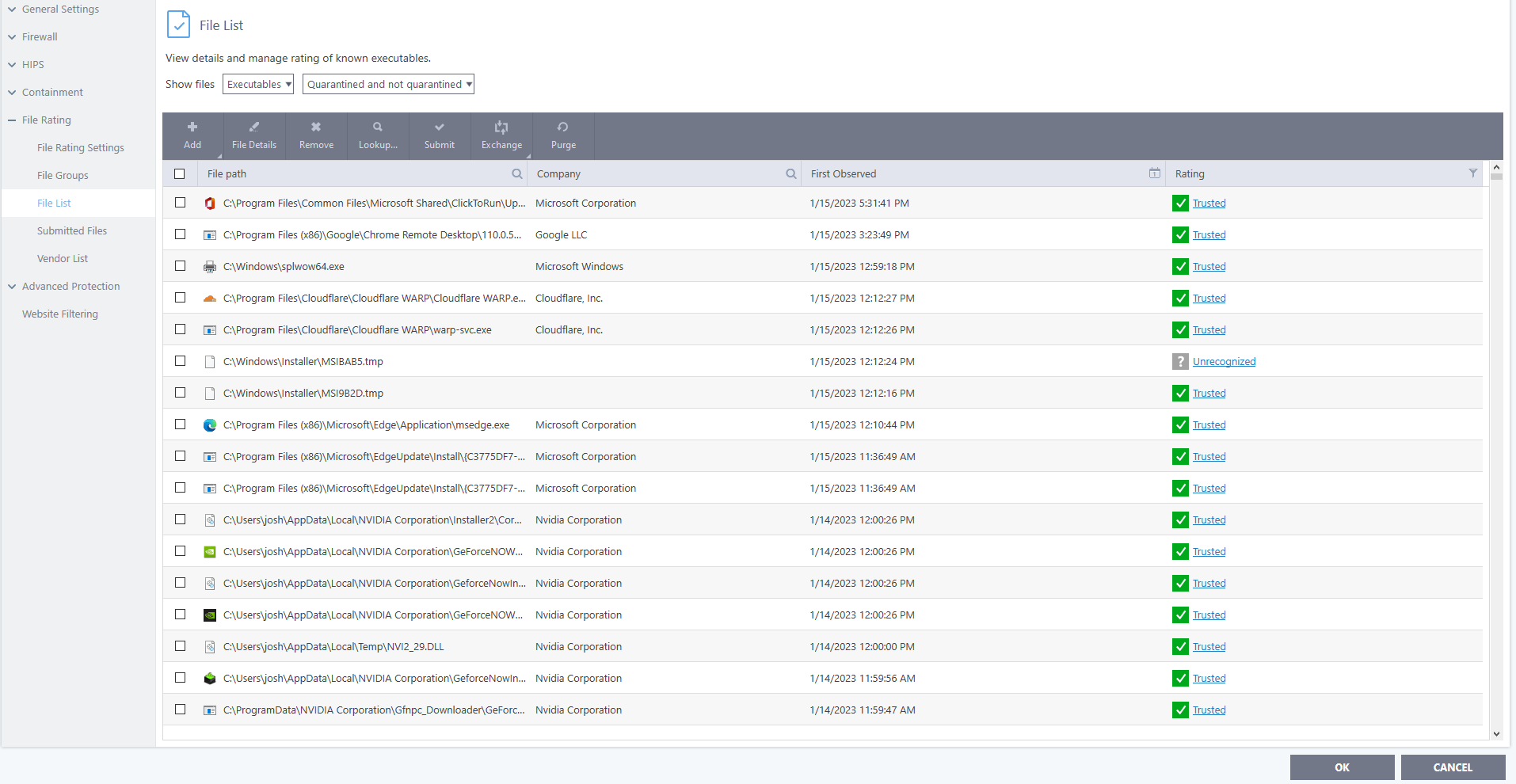
Програмата е проектирана да работи автоматично, без да е необходима човешка намеса. Тя следи мрежовите връзки и блокира всеки подозрителен или нежелан трафик въз основа на правилата и настройките, които са конфигурирани. Потребителите могат да персонализират настройките на програмата по свой вкус и също така предлага предупреждения и известия, когато бъде открита подозрителна дейност.

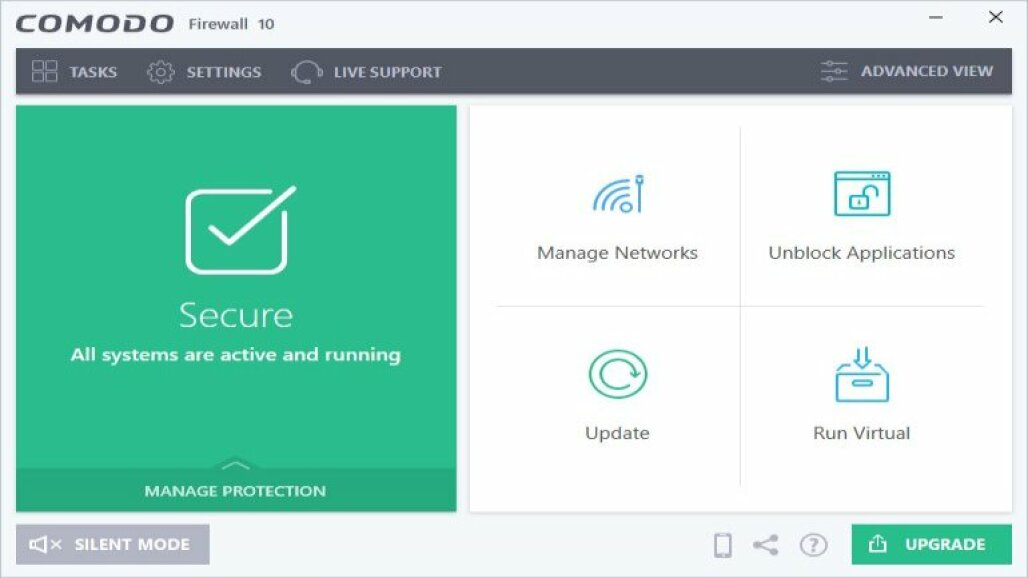
В сравнение с други програми за защитна стена, ZoneAlarm обикновено се счита за по-модерно и цялостно решение. Въпреки това, производителността и ефективността на програмата може да зависи от различни фактори, като специфичните функции и настройки, които се използват, и видовете заплахи, които са насочени.

**Comodo Firewall.** Това е предимно защитна стена но с повече функции. Comodo Firewall е безплатен и мощен софтуер, предназначен да защитава вашия компютър от неоторизиран достъп и да контролира потока на входящия и изходящия мрежов трафик. Той следи и контролира мрежовите връзки на вашия компютър, като блокира всеки подозрителен или нежелан трафик, за да предпази системата ви от зловреден софтуер, хакери и опити за фишинг. Comodo Firewall се предлага с различни функции, които подобряват сигурността на вашия компютър. Някои от функциите му включват:

* Двупосочна защитна стена, която следи както входящия, така и изходящия трафик
* Разширена защита при изтегляне, която сканира файловете за злонамерен софтуер, преди да бъдат изтеглени
* Автоматични актуализации, за да се гарантира, че програмата е винаги актуална
* Система за предотвратяване на проникване на хост (HIPS), която следи системата за всякакви злонамерени действия и я блокира
* Автоматично тестване на неизвестни програми за защита на вашата система от нови неизвестни заплахи
* Функция за режим на игра, която позволява на потребителите да играят игри без прекъсвания

Comodo Firewall прави всичко, което една лична защитна стена трябва да прави, като прикрива портове срещу външни атаки и предотвратява изтичането отвътре от програми, злоупотребяващи с вашата интернет връзка. В допълнение, предлага тестова среда, защитен браузър, HIPS, оценка на файловете въз основа на репутация и др.





Comodo Firewall има оценка на файлове, която проверява файловете спрямо облачната база данни на Comodo, когато имате достъп до тях и казва дали файлът е верифициран. Ако базата данни идентифицира процес като злонамерен софтуер или като потенциално нежелана програма, Comodo прекратява процеса и извежда известие. Освен това получавате изскачащ прозорец, предлагащ услуги на GeekBuddy. Оценката на файлове също е функция на антивирусната програма, че други защитни слоеве винаги се включват, преди оценката на файлове да има шанс.

**pfSense** е безплатен софтуер за защитна стена с отворен код, който може да се използва за защита на мрежи от различни киберзаплахи. Базиран е на операционната система FreeBSD и е специално проектиран да се използва като защитна стена и рутер. Той е известен със своята гъвкавост и мащабируемост, може да се използва за дома, малък и голям бизнес, както и за корпоративни среди.

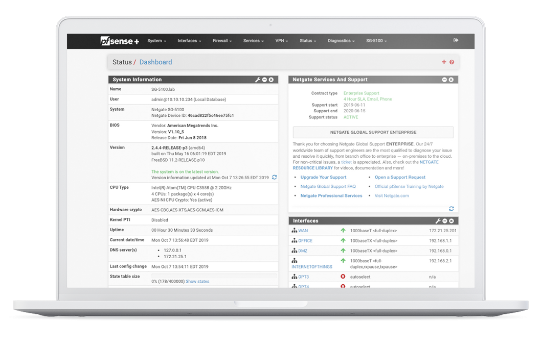
pfSense предоставя широк набор от функции, включително:

* Защитна стена за филтриране на пакети със състояние
* VPN поддръжка (IPsec, OpenVPN и L2TP)
* Сървър на Dynamic Host Configuration Protocol (DHCP).
* Система за пренасочване на домейн имена (DNS).
* Качество на услугата (QoS) за управление на честотната лента
* Captive портал за мрежи за гости
* Разширено оформяне на трафика
* Инструменти за отчитане и наблюдение

Едно от най-добрите неща за pfSense е неговата гъвкавост и мащабируемост. Може да се използва за широк спектър от среди, от малки домашни мрежи до големи корпоративни мрежи. Може да се инсталира на стандартен x86-64 хардуер, като виртуална машина или в облачна среда, което го прави адаптивен към различни нужди и инфраструктури.

Друго ключово предимство на pfSense е неговата широка гама от функции. Той предоставя разширени функции като защитна стена за филтриране на пакети, поддръжка на VPN, DHCP сървър, DNS пренасочване, качество на услугата (QoS) за управление на честотната лента, портал за прихващане за мрежи за гости, усъвършенствано оформяне на трафика и инструменти за отчитане и наблюдение. Тези функции го правят цялостно решение за мрежова сигурност и управление, което може да помогне за защита срещу широк набор от кибер заплахи и да управлява ефективно мрежовия трафик.

Освен това pfSense е софтуер с отворен код, което означава, че може да бъде свободно изтеглен, използван и модифициран от всеки. Това позволява на потребителите да персонализират софтуера, за да отговаря на техните специфични нужди, а също и да се възползват от приноса на голямата общност от разработчици и потребители, които непрекъснато работят върху софтуера.



**GlassWire Firewall** е GlassWire е програма за защитна стена, която е предназначена да предпазва компютъра от неоторизиран достъп и да наблюдава мрежовата активност. Предлага се за операционни системи Windows и има версия за Android.

GlassWire осигурява наблюдение на мрежата в реално време, което позволява на потребителите да виждат цялата мрежова активност на своя компютър в лесен за разбиране визуален формат. Той също така включва функции като:

* Двупосочна защитна стена, която следи както входящия, така и изходящия трафик
* Сигнали за мрежова сигурност, които уведомяват потребителите за подозрителна дейност
* Отдалечен достъп и управление, така че потребителите да могат да контролират своята защитна стена отвсякъде.
* Монитор за използване на честотната лента, който позволява на потребителите да проследяват използването на интернет и да задават предупреждения за използване
* Функция „Правила на защитната стена“, която дава на потребителите повече контрол върху тяхната мрежова сигурност, като им позволява да създават персонализирани правила за конкретни приложения или IP адреси
* Мониторинг на мрежовата активност на приложения и услуги, които работят на компютъра.

Защитната стена на GlassWire е проектирана да работи автоматично, без необходимост от човешка намеса, тя също така включва функция „Искане за свързване“, която подканва потребителите за разрешение, преди да позволи на нови приложения да се свързват с интернет, което може да осигури допълнителен слой сигурност.

В допълнение, чистият и удобен за потребителя интерфейс на GlassWire улеснява потребителите да разбират и управляват своята мрежова активност.

Графичният потребителски интерфейс (GUI) на GlassWire е проектиран да бъде удобен за потребителя и лесен за навигация. Основното табло за управление показва емисия на живо за цялата мрежова активност на компютъра, включително входящи и изходящи връзки и използване на честотна лента. Тази информация е представена в ясен и стегнат визуален формат, което улеснява потребителите да разберат какво се случва в тяхната мрежа.

GUI също така включва няколко раздела, които осигуряват достъп до различни функции и настройки. Разделът „Предупреждения“ показва списък с всички предупреждения за сигурност, които са били генерирани от защитната стена, включително информация за източника на предупреждението и типа дейност, която го е задействала.

Разделът "Защитна стена" дава на потребителите повече контрол върху тяхната мрежова сигурност, като им позволява да създават персонализирани правила за конкретни приложения или IP адреси. Потребителите могат също така да видят списък с всички приложения, които са били блокирани от защитната стена, и да изберат да ги деблокират.

Разделът „Широчина на честотната лента“ показва графично представяне на използването на интернет от компютъра във времето, което може да бъде полезно за идентифициране на тенденции и задаване на предупреждения за използване.

Разделът „Приложения“ показва списък с всички приложения и услуги, които се изпълняват на компютъра и тяхната мрежова активност, което позволява на потребителите да наблюдават и контролират мрежовата активност на конкретни приложения.

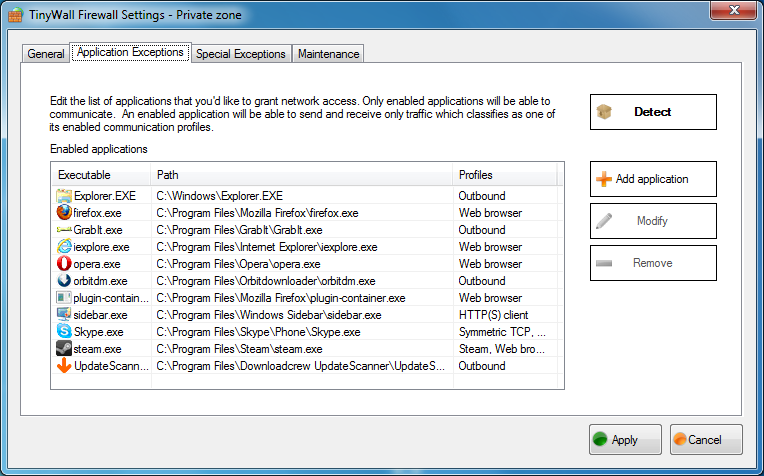
Картина, която съдържа текст

Описанието е генерирано автоматичноКартина, която съдържа текст, екранна снимка, електроника, дисплей

Описанието е генерирано автоматичноКато цяло GUI на GlassWire е проектиран да улесни потребителите да наблюдават и управляват своята мрежова активност, да преглеждат предупреждения за сигурност и да контролират настройките на защитната стена. Интерфейсът е интуитивен и лесен за използване, с ясна и кратка информация, представена по визуално приятен начин.

**TinyWall** е безплатна, лека програма за защитна стена за операционни системи Windows. Той е проектиран да бъде лесен за използване и лесен за разбиране, като същевременно предоставя разширени функции за защита на компютъра от неоторизиран достъп и контролиране на потока от входящ и изходящ мрежов трафик. Потребителският интерфейс на TinyWall е прост и лесен за навигация, той е проектиран да бъде минималистичен и фокусиран върху най-важните опции и настройки. Тя няма същото ниво на сложност и опции като другите защитни стени, но е предназначена да бъде проста и лесна за използване, подходяща за домашни потребители и малки фирми.

TinyWall включва функции като:

* Двупосочна защитна стена, която следи както входящия, така и изходящия трафик
* Автоматичен режим на обучение, който позволява на защитната стена да научи поведението на мрежата и автоматично да създава правила
* Възможност за блокиране на всички входящи връзки, с изключение на тези, които са изрично разрешени
* Възможност за разрешаване на всички изходящи връзки, с изключение на тези, които са изрично блокирани
* Функция за бял списък, която позволява на потребителите да създават списък с надеждни приложения и IP адреси
* Режим "заключване", който може да се използва за бързо блокиране на всички входящи връзки
* Опция за защита с парола на настройките на защитната стена за предотвратяване на неоторизирани промени

TinyWall е добър избор за тези, които търсят лека, лесна за използване програма за защитна стена, която може да помогне за защита на компютъра им от неоторизиран достъп и да контролира потока на мрежовия трафик. Неговият автоматичен режим на обучение и лесен за използване интерфейс го правят добър вариант за по-малко технически потребители или тези, които не се нуждаят от разширени функции.