****

МЕЖСЕТЕВЫЕ ЭКРАНЫ

1. PFSENSE

Это решение для обеспечения безопасности с открытым исходным кодом на основе ядра FreeBSD. pfSense – это один из ведущих сетевых файрволов с коммерческим уровнем функционала.

Бесплатно вы получаете общую версию.

Мне нравится их исчерпывающая документация (https://doc.pfsense.org/index.php/Main_Page), хорошо понятная и простая в использовании. Вот некоторые из значимых упоминаемых особенностей pfSense:

файрвол — фильтрация IP/портов, ограничение соединений, работа на канальном уровне, нормализация пакетов;

таблица состояний — по умолчанию все правила находятся в отслеживаемом состоянии, множественные конфигураций подходят для обработки состояний;

серверная балансировка нагрузки — встроенный балансировщик нагрузки для ее распределения между несколькими серверами;

NAT (преобразование сетевых адресов) — переадресация портов, отражение;

HA (высокая доступность) — переход на вторичный сервер, если основной дал сбой;

мульти-WAN (глобальная компьютерная сеть) – использование более чем одного интернет-соединения;

VPN (виртуальная частная сеть) — поддержка IPsec и OpenVPN;

создание отчетов – сохранение информации об использованных ресурсах;

мониторинг – мониторинг в режиме реального времени;

динамический DNS – включено несколько DNS-клиентов;

поддержка DHCP Relay.

Больше функций, чем предоставляют некоторые коммерческие файрволы, вы получаете БЕСПЛАТНО.

Кроме того, у вас также есть возможность устанавливать пакеты всего одним щелчком мыши.

Например:

безопасность — stunner, snort, tinc, nmap, arpwatch;

мониторинг – iftop, ntopng, softflowd, urlsnarf, darkstat, mailreport;

создание сети — netio, nut, Avahi;

маршрутизация — frr, olsrd, routed, OpenBGPD;

обслуживание — iperf, widentd, syslog-ng, bind, acme, imspector, git, dns-server.

pfSense выглядит многообещающе и его стоит попробовать.

2. IPFire

Основан на Netfilter и ему доверяют тысячи компаний по всему миру.

IPFire можно использовать как файерволл, прокси-сервер или VPN-шлюз — все зависит от того, как вы настроите его. Он обладает большой гибкостью в настройках.

IDS (система обнаружения вторжений) является встроенной, поэтому атаки обнаруживаются и предотвращаются с самого начала, а с помощью дополнения Guardian вы можете осуществлять автоматическую профилактику.

Вы сможете понять как работать с IPFire менее чем за 30 минут. Прочитать больше о его возможностях можно здесь (https://www.ipfire.org/features)

www.ipfire.org (https://www.ipfire.org/features)

3 OPNSense

Является ответвлением pfSense и m0n0wall. Графический интерфейс доступен на нескольких языках, таких как французский, китайский, японский, итальянский, русский и др.

OPNSense обладает многими серьезными уровнями безопасности и функциями файрвола, такими как IPSec, VPN, 2FA, QoS, IDPS, Netflow, Proxy, Webfilter и т.д.

Он совместим с 32-битной или 64-битной системной архитектурой и доступен для загрузки как ISO-образ и USB-установщик.

https://opnsense.org/

4. NG Firewall от Untangle

Это единая платформа, где вы можете получить все необходимое для защиты сети своей организации. https://www.untangle.com/

Он обладает красивой панелью инструментов, попробовать демо-версию можно здесь (http://demo.untangle.com/admin/index.do) . Он работает как магазин приложений, где вы можете запускать или отключать отдельные приложения (модули) в соответствии со своими потребностями.

В бесплатной версии вы получаете доступ к самой платформе NG Firewall, бесплатные приложения и 14-дневную пробную версию платных функций.

Untangle (https://www.untangle.com /)

5. Smoothwall express

Это бесплатное решение с простым веб-интерфейсом для настройки и управления файрволом.

Smoothwall express поддерживает LAN (локальную сеть), DMZ (демилитаризованную зону), внутренний и внешний сетевой файрвол, веб-прокси для ускорения, статистику трафика и др.
Выключение или перезагрузка возможны непосредственно через веб-интерфейс.

http://www.smoothwall.org/

6. ufw (несложный файрвол)

Работает с Ubuntu. Для управления системой фильтрации пакетов ядра Linux (Netfilter) он использует интерфейс командной строки.

https://launchpad.net/ufw

7. csf (ConfigServer security)

Протестирован и поддерживается на следующих OS и виртуальных серверах:

RHEL/CentOS
CloudLinux
Fedora
OpenSUSE
Debian
Ubuntu
Slackware
OpenVZ
KVM
VirtualBox
XEN
VMware
Virtuozzo
UML

csf — это файрвол с контролем состояния соединений, обнаружением входа в систему и обеспечением безопасности для серверов Linux.

https://www.configserver.com/cp/csf.html

****

АНТИВИРУСЫ

1. **Armadito Antivirus - https://armadito.com**
2. **OpenAntiVirus Project - http://www.openantivirus.org**
3. **ClamAV - https://www.talosintelligence.com/clamav**
4. **ClamWin - http://www.clamwin.com**
5. **Moon Secure AV - https://moon-secure-antivirus.en.softonic.com**

Также Статьи по bypass

1. **Обход антивируса с помощью C #. https://codeby.net/threads/av-bypass-s-pomoschju-c.58637**
2. **Обход антивируса (Reverse Python Shell) 100% FUD https://codeby.net/threads/obxod-antivirusa-reverse-python-shell-100-fud.58426**
3. **Обход антивируса с помощью ctypes (python) https://codeby.net/threads/obxod-antivirusa-s-pomoschju-ctypes-python.58449**
4. **Обход антивирусов. Антиэмуляция, обход сигнатур и все все все. Часть III. https://codeby.net/threads/obxod-antivirusov-antiehmuljacija-obxod-signatur-i-vse-vse-vse-chast-iii.59751**
5. **Обход антивирусов. Антиэмуляция, обход сигнатур и все все все. Часть I. https://codeby.net/threads/obxod-antivirusov-antiehmuljacija- obxod-signatur-i-vse-vse-vse-chast-i.5973**