Network Security

R.M.K.A.B. Werellagama

- *Port and Vulnerability scanning*
- *Open Source Custom Router Firmware*
- *Firewalls*
- *Dynamic Packet Filtering*
- *Firewall Bypassing Methods and Techniques*
- *Network Attacks*
- *Effective Network Isolation*
- *Network Monitoring for Threats*
- *RSYSLOG*
- *Malware and Hackers*
- *How We Are Tracked Online*
- *Search Engines and Privacy*
- *Google keeps your searches and other identifiable user information for an undefined period of time Discussion*
- *Passwords and Authentication Methods*
- *Hashdumps and Passwords*
- *Password security*

Port and Vulnerability scanning

A List of Common Default Router IP Addresses

Router Brand	Common Default IP Addresses
2Wire	192.168.1.1 192.168.0.1 192.168.1.254 10.0.0.138
3Com	192.168.1.1 192.168.1.10.1
Actiontec	192.168.1.1 192.168.0.1 192.168.2.1 192.168.254.254
Airlink	192.168.1.1 192.168.2.1
Airlive	192.168.2.1
Airties	192.168.2.1
Apple	10.0.1.1
Amped Wireless	192.168.3.1
Asus	192.168.1.1 192.168.2.1 10.10.1.1
Aztech	192.168.1.1 192.168.2.1 192.168.1.254 192.168.254.254

Belkin	192.168.1.1 192.168.2.1 10.0.0.2 10.1.1.1
Billion	192.168.1.254 10.0.0.2
Buffalo	192.168.1.1 192.168.11.1
Dell	192.168.1.1
Cisco	192.168.1.1 192.168.0.30 192.168.0.50 10.0.0.1 10.0.0.2
D-Link	192.168.1.1 192.168.0.1 192.168.0.10 192.168.0.101 192.168.0.30 192.168.0.50 192.168.1.254 192.168.15.1 192.168.254.254 10.0.0.1 10.0.0.2 10.1.1.1 10.90.90.90
Edimax	192.168.2.1
Eminent	192.168.1.1 192.168.0.1 192.168.8.1
Gigabyte	192.168.1.254

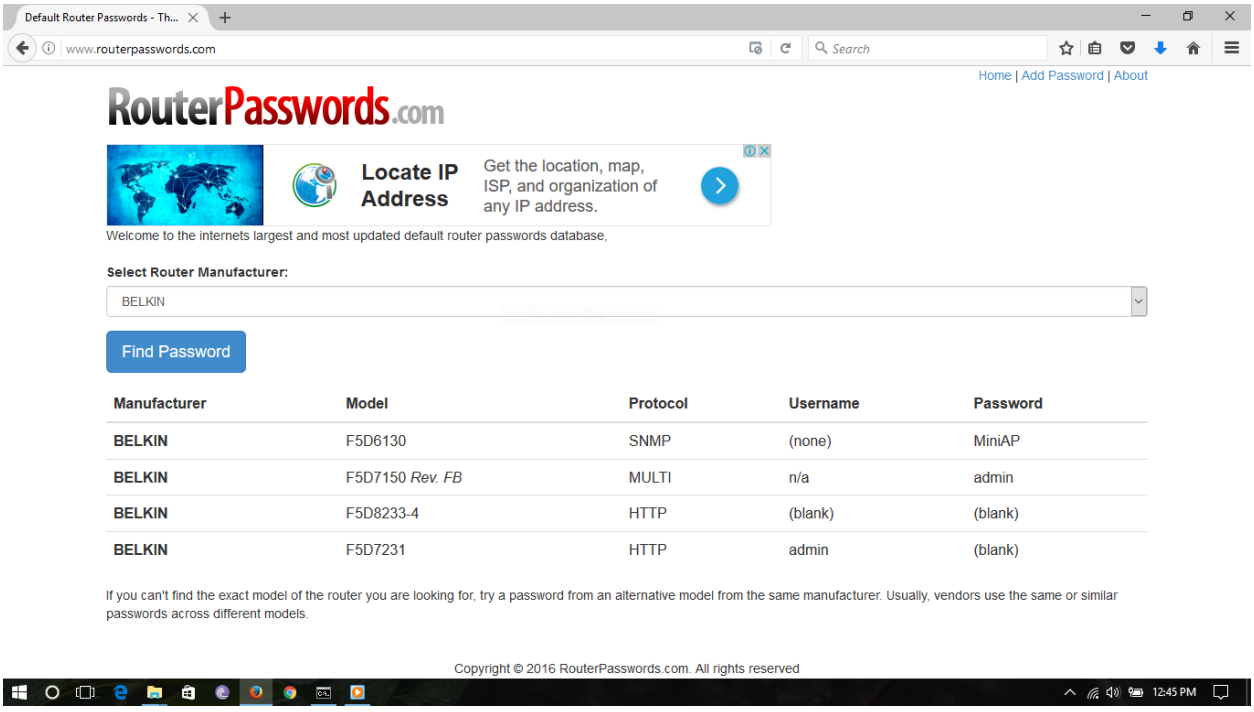
Hawking	192.168.1.200 192.168.1.254
Huawei	192.168.1.1 192.168.0.1 192.168.3.1 192.168.8.1 192.168.100.1 10.0.0.138
LevelOne	192.168.0.1 192.168.123.254
Linksys	192.168.1.1 192.168.0.1 192.168.1.10 192.168.1.210 192.168.1.254 192.168.1.99 192.168.15.1 192.168.16.1 192.168.2.1
Microsoft	192.168.2.1
Motorola	192.168.0.1 192.168.10.1 192.168.15.1 192.168.20.1 192.168.30.1 192.168.62.1 192.168.100.1 192.168.102.1 192.168.1.254
MSI	192.168.1.254
Netgear	192.168.0.1 192.168.0.227
NetComm	192.168.1.1 192.168.10.50

	192.168.20.1 10.0.0.138
Netopia	192.168.0.1 192.168.1.254
Planet	192.168.1.1 192.168.0.1 192.168.1.254
Repotec	192.168.1.1 192.168.10.1 192.168.16.1 192.168.123.254
Senao	192.168.0.1
Siemens	192.168.1.1 192.168.0.1 192.168.1.254 192.168.2.1 192.168.254.254 10.0.0.138 10.0.0.2
Sitecom	192.168.0.1 192.168.1.254 192.168.123.254 10.0.0.1
SMC Networks	192.168.1.1 192.168.0.1 192.168.2.1 10.0.0.1 10.1.10.1
Sonicwall	192.168.0.3 192.168.168.168
SpeedTouch	10.0.0.138 192.168.1.254

Sweex	192.168.15.1 192.168.50.1 192.168.55.1 192.168.251.1
Tenda	192.168.1.1 192.168.0.1
Thomson	192.168.0.1 192.168.1.254 192.168.100.1
TP-Link	192.168.1.1 192.168.0.1 192.168.0.254
Trendnet	192.168.1.1 192.168.0.1 192.168.0.30 192.168.0.100 192.168.1.100 192.168.1.254 192.168.10.1 192.168.10.10 192.168.10.100 192.168.2.1 192.168.223.100 200.200.200.5
U.S. Robotics	192.168.1.1 192.168.2.1 192.168.123.254
Zoom	192.168.1.1 192.168.2.1 192.168.4.1 192.168.10.1 192.168.1.254 10.0.0.2 10.0.0.138
ZTE	192.168.1.1 192.168.0.1

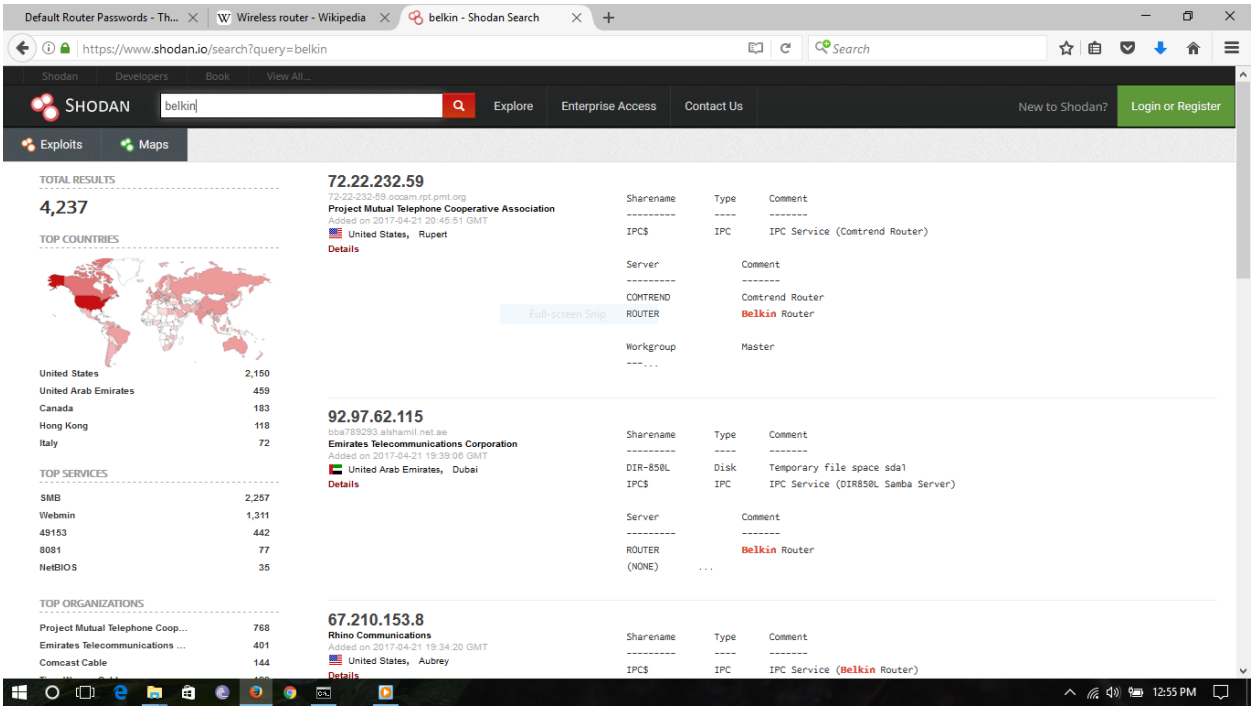
	192.168.100.100 192.168.1.254 192.168.2.1 192.168.2.254
Zyxel	192.168.1.1 192.168.0.1 192.168.2.1 192.168.4.1 192.168.10.1 192.168.1.254 192.168.254.254 10.0.0.2 10.0.0.138

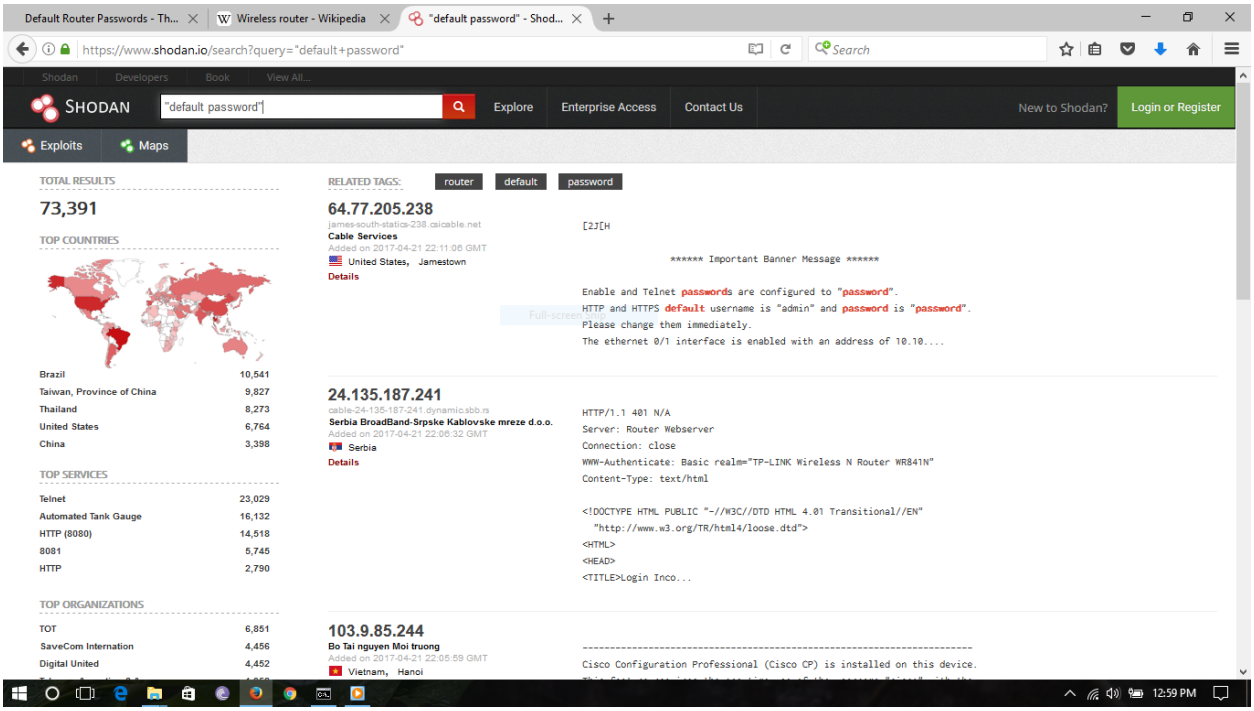
RouterPassword.com



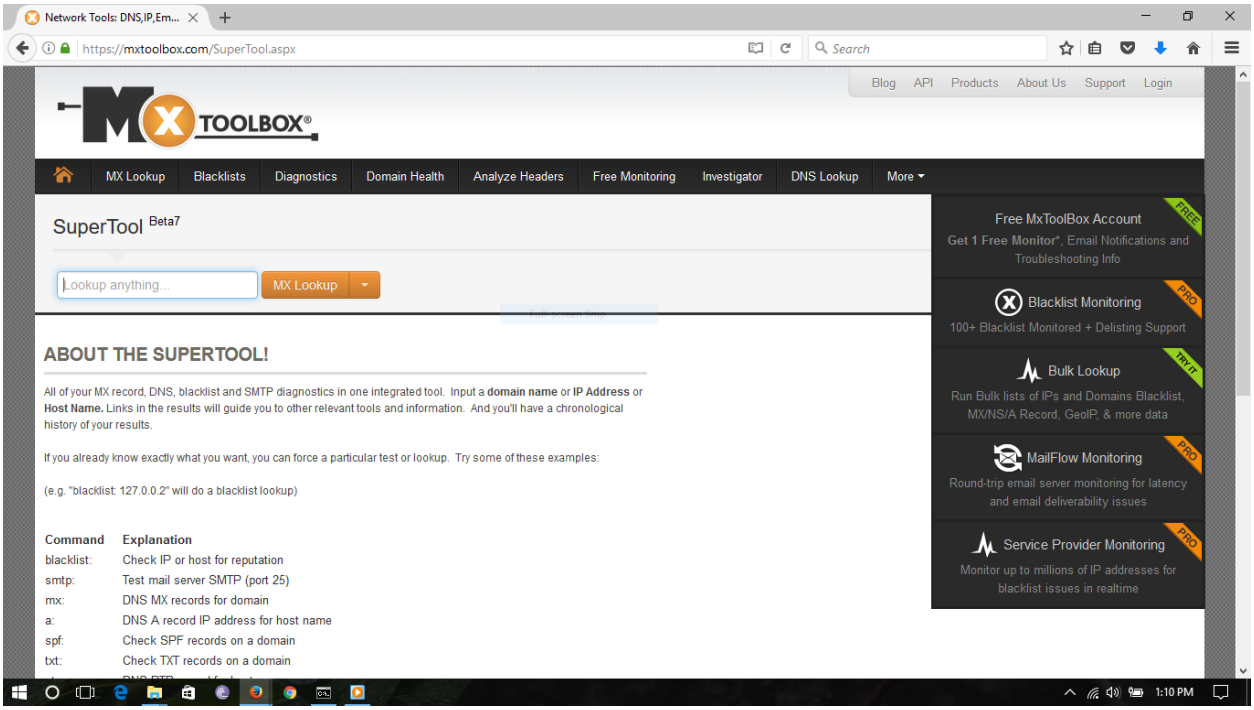
External Vulnerability Scanning tools

Shodan

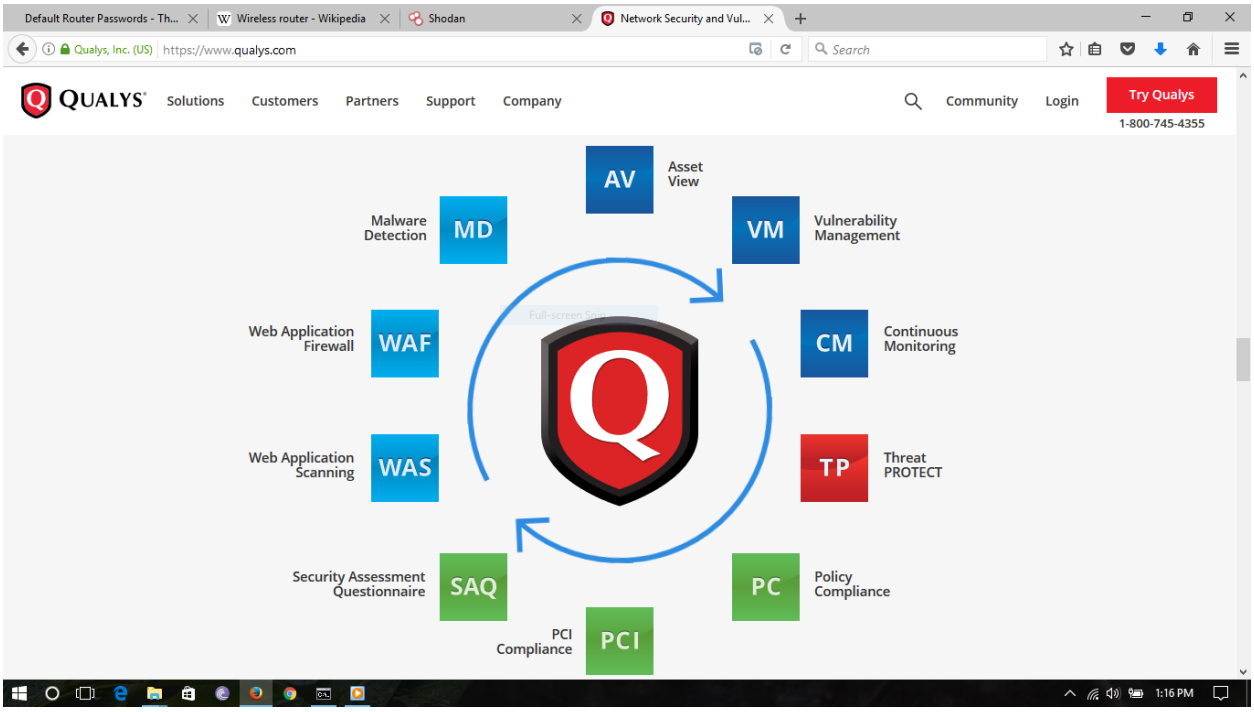




Mxtoolbox



Qualys

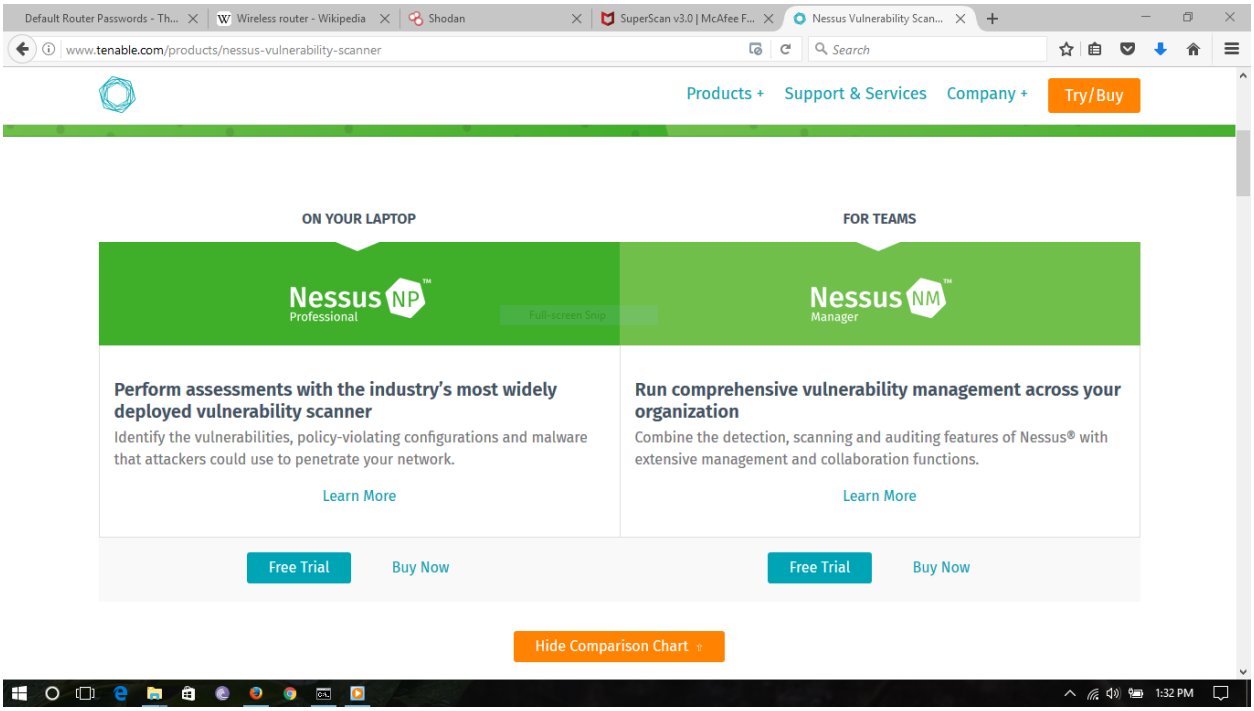


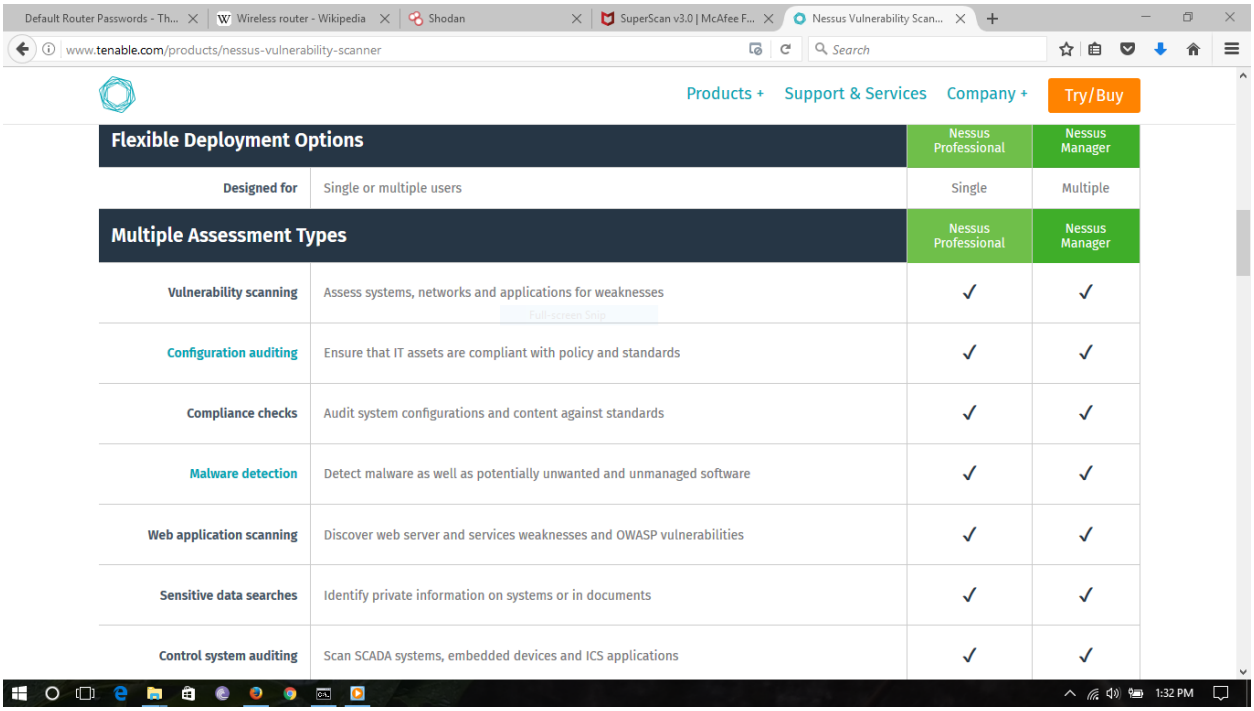
Internal Vulnerability Scanning tools

Microsoft Baseline Security Analyzer

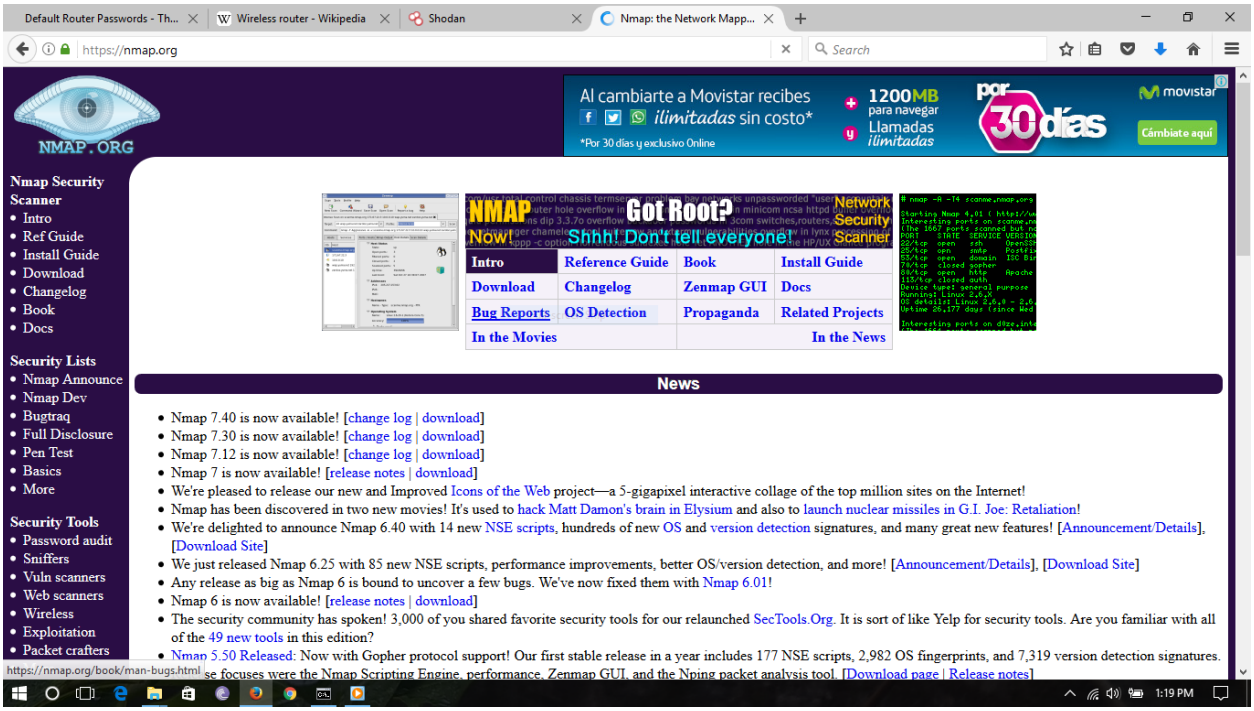
Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings. Security updates are determined by the current version of MBSA using the Windows Update Agent present on Windows computers since Windows 2000 Service Pack 3. The less-secure settings, often called Vulnerability Assessment (VA) checks, are assessed based on a hard-coded set of registry and file checks. An example of a VA might be that permissions for one of the directories in the /www/root folder of IIS could be set at too low a level, allowing unwanted modification of files from outsiders.

Nessus

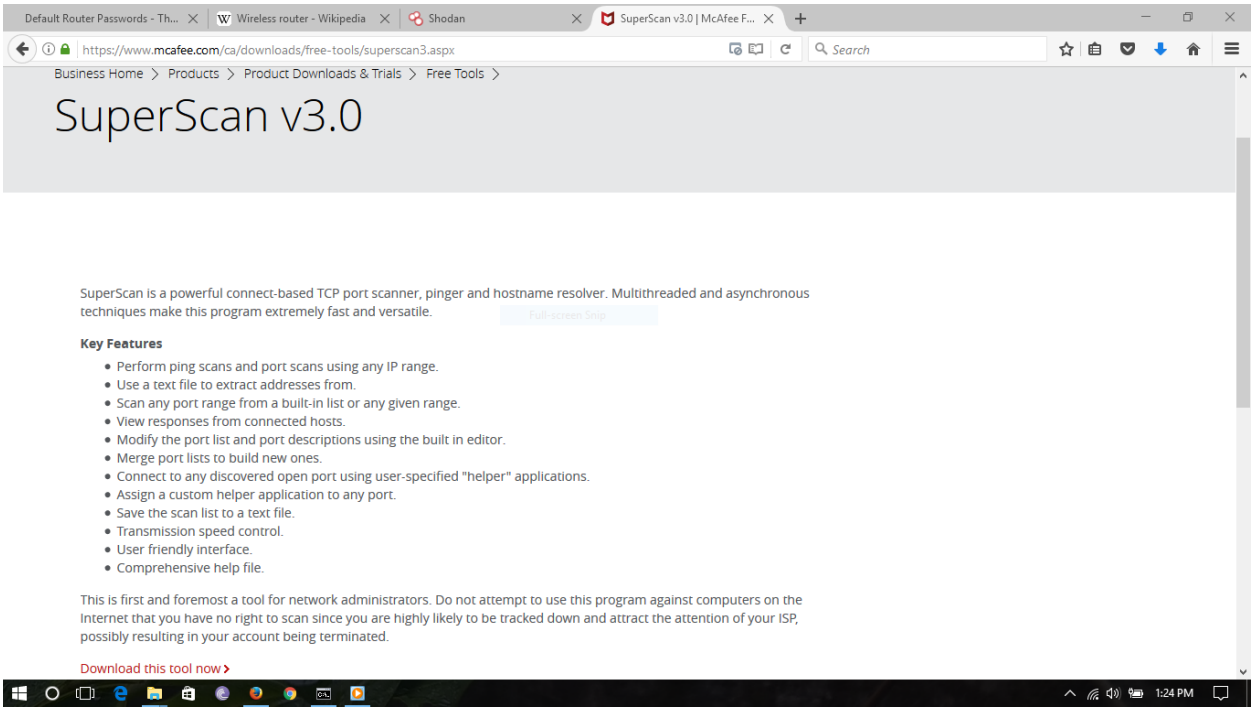



Default Router Passwords - Th...
Wireless router - Wikipedia
Shodan
SuperScan v3.0 | McAfee F...
Nessus Vulnerability Scan...
www.tenable.com/products/nessus-vulnerability-scanner
Search
Products +
Support & Services
Company +
Try/Buy
Flexible Deployment Options
Nessus Professional
Nessus Manager
Designed for
Single or multiple users
Single
Multiple
Multiple Assessment Types
Nessus Professional
Nessus Manager
Vulnerability scanning
Assess systems, networks and applications for weaknesses
Configuration auditing
Ensure that IT assets are compliant with policy and standards
Compliance checks
Audit system configurations and content against standards
Malware detection
Detect malware as well as potentially unwanted and unmanaged software
Web application scanning
Discover web server and services weaknesses and OWASP vulnerabilities
Sensitive data searches
Identify private information on systems or in documents
Control system auditing
Scan SCADA systems, embedded devices and ICS applications
1:32 PM

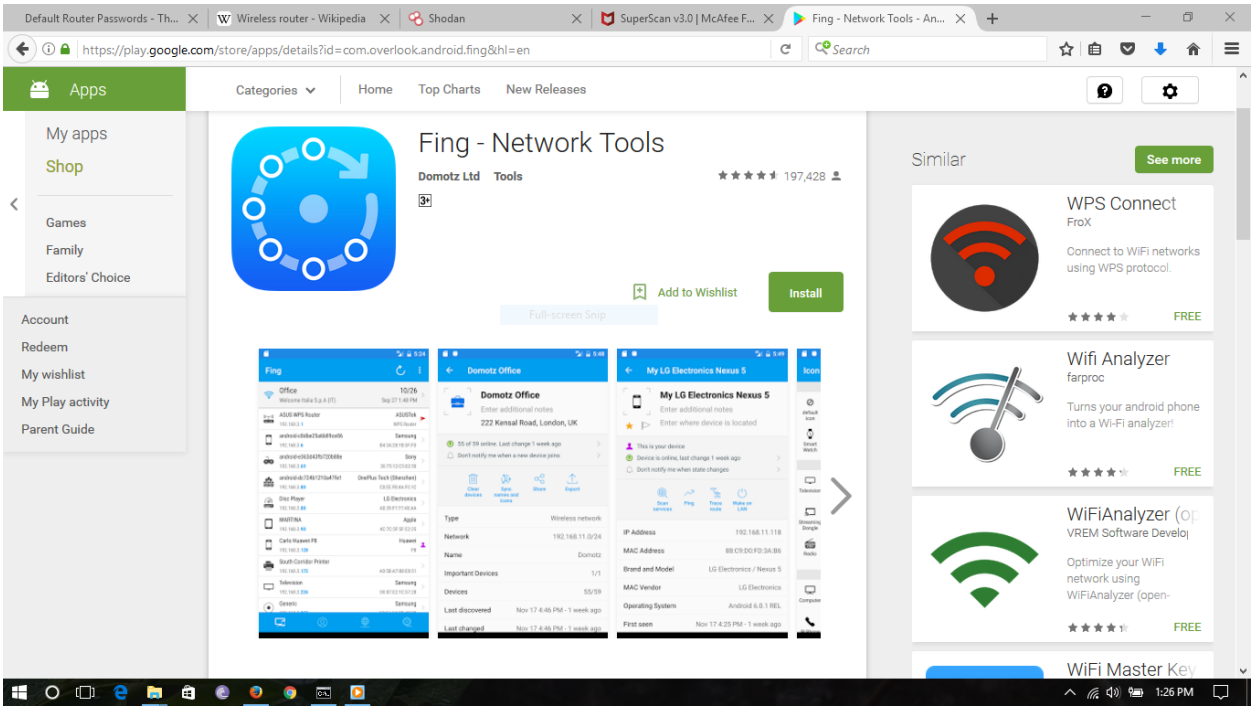
Nmap

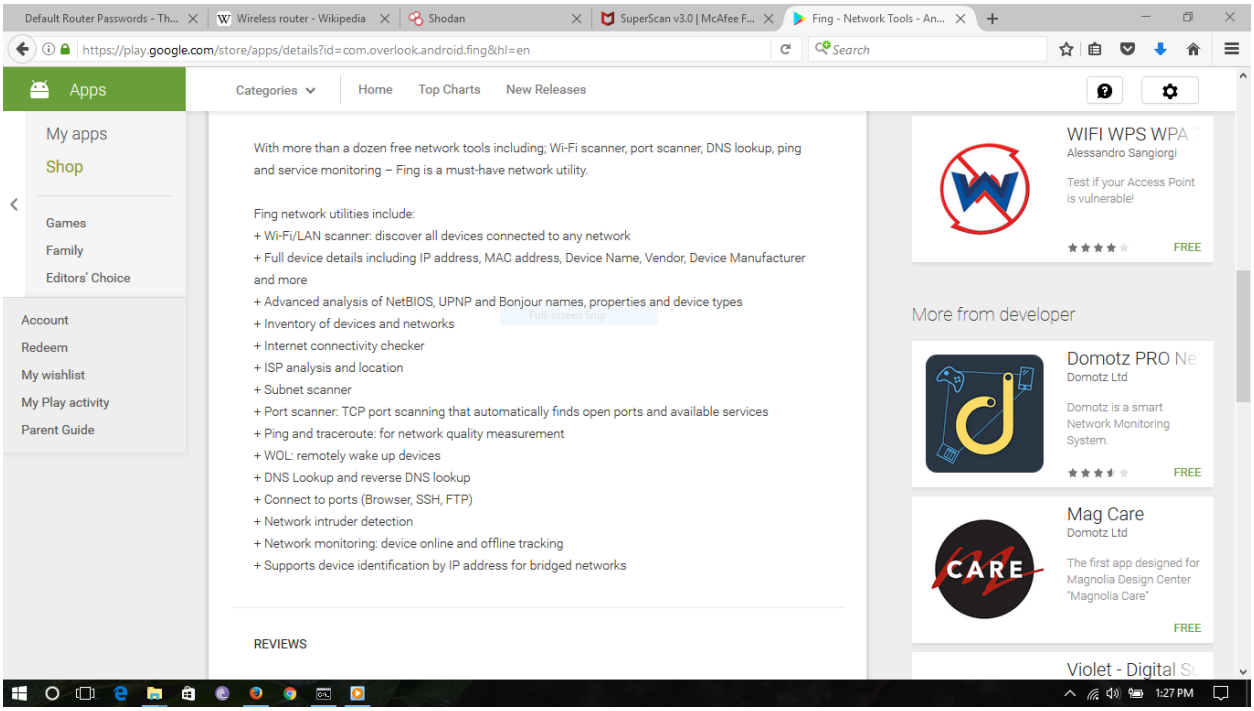

Default Router Passwords - Th...
Wireless router - Wikipedia
Shodan
Nmap: the Network Mapp...
https://nmap.org
Search
NMAP.ORG
Al cambiarte a Movistar recibes ilimitadas sin costo*
*Por 30 días y exclusivo Online
1200MB para navegar
Llamadas ilimitadas
por 30 días
movistar
Cámbiate aquí
Nmap Security Scanner
Intro
Ref Guide
Install Guide
Download
Changelog
Book
Docs
Security Lists
Nmap Announce
Nmap Dev
Bugtraq
Full Disclosure
Pen Test
Basics
More
Security Tools
Password audit
Sniffers
Vuln scanners
Web scanners
Wireless
Exploitation
Packet crafters
NMAP Got Root? Network Security Scanner
Now! Shhh! Don't tell everyone!
Intro
Reference Guide
Book
Install Guide
Download
Changelog
Zenmap GUI
Docs
Bug Reports
OS Detection
Propaganda
Related Projects
In the Movies
In the News
News
Nmap 7.40 is now available! [change log | download]
Nmap 7.30 is now available! [change log | download]
Nmap 7.12 is now available! [change log | download]
Nmap 7 is now available! [release notes | download]
We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!
Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!
We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [Announcement/Details], [Download Site]
We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Announcement/Details], [Download Site]
Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
Nmap 6 is now available! [release notes | download]
The security community has spoken! 3,000 of you shared favorite security tools for our relaunched SecTools.Org. It is sort of like Yelp for security tools. Are you familiar with all of the 49 new tools in this edition?
Nmap 5.50 Released: Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures.
https://nmap.org/book/man-bugs.html
1:19 PM

Mcafee


Default Router Passwords - Th...
Wireless router - Wikipedia
Shodan
SuperScan v3.0 | McAfee F...
https://www.mcafee.com/ca/downloads/free-tools/superscan3.aspx
Search
Business Home > Products > Product Downloads & Trials > Free Tools >
SuperScan v3.0
SuperScan is a powerful connect-based TCP port scanner, pinger and hostname resolver. Multithreaded and asynchronous techniques make this program extremely fast and versatile.
Key Features
Perform ping scans and port scans using any IP range.
Use a text file to extract addresses from.
Scan any port range from a built-in list or any given range.
View responses from connected hosts.
Modify the port list and port descriptions using the built in editor.
Merge port lists to build new ones.
Connect to any discovered open port using user-specified "helper" applications.
Assign a custom helper application to any port.
Save the scan list to a text file.
Transmission speed control.
User friendly interface.
Comprehensive help file.
This is first and foremost a tool for network administrators. Do not attempt to use this program against computers on the Internet that you have no right to scan since you are highly likely to be tracked down and attract the attention of your ISP, possibly resulting in your account being terminated.
Download this tool now
1:24 PM

Fing


Default Router Passwords - Th...
Wireless router - Wikipedia
Shodan
SuperScan v3.0 | McAfee F...
Fing - Network Tools - An...
https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=en
Search
Apps
Categories
Home
Top Charts
New Releases
My apps
Shop
Games
Family
Editors' Choice
Account
Redeem
My wishlist
My Play activity
Parent Guide
Fing - Network Tools
Domotz Ltd
Tools
197,428
3+
Add to Wishlist
Install
Similar
See more
WPS Connect
FroX
Connect to WiFi networks using WPS protocol.
FREE
Wifi Analyzer
farproc
Turns your android phone into a Wi-Fi analyzer!
FREE
WiFiAnalyzer
VREM Software Develo
Optimize your WiFi network using WiFiAnalyzer (open-
FREE
WiFi Master Key
1:26 PM


Default Router Passwords - Th...
Wireless router - Wikipedia
Shodan
SuperScan v3.0 | McAfee F...
Fing - Network Tools - An...
https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=en
Search
Apps
Categories
Home
Top Charts
New Releases
My apps
Shop
Games
Family
Editors' Choice
Account
Redeem
My wishlist
My Play activity
Parent Guide
With more than a dozen free network tools including; Wi-Fi scanner, port scanner, DNS lookup, ping and service monitoring – Fing is a must-have network utility.
Fing network utilities include:
+ Wi-Fi/LAN scanner: discover all devices connected to any network
+ Full device details including IP address, MAC address, Device Name, Vendor, Device Manufacturer and more
+ Advanced analysis of NetBIOS, UPNP and Bonjour names, properties and device types
+ Inventory of devices and networks
+ Internet connectivity checker
+ ISP analysis and location
+ Subnet scanner
+ Port scanner: TCP port scanning that automatically finds open ports and available services
+ Ping and traceroute: for network quality measurement
+ WOL: remotely wake up devices
+ DNS Lookup and reverse DNS lookup
+ Connect to ports (Browser, SSH, FTP)
+ Network intruder detection
+ Network monitoring: device online and offline tracking
+ Supports device identification by IP address for bridged networks
REVIEWS
WIFI WPS WPA
Alessandro Sangiorgi
Test if your Access Point is vulnerable!
FREE
More from developer
Domotz PRO Ne
Domotz Ltd
Domotz is a smart Network Monitoring System.
FREE
Mag Care
Domotz Ltd
The first app designed for Magnolia Design Center "Magnolia Care"
FREE
Violet - Digital S
1:27 PM

Open Source Custom Router Firmware

List of router firmware projects

This is a list of notable custom-firmware projects for wireless routers or software distributions for PC-based routers that have been created and are maintained by people and groups other than the manufacturer of the product. Many of these will run on various brands of Linux-based devices, such as Linksys, Asus, Netgear, etc. The extent of support for (and testing on) particular hardware varies from project to project.

1. OpenWrt – Customizable FOSS firmware written from scratch; features a combined SquashFS/JFFS2 file system and the package manager opkg with over 3000 available packages (Linux/GPL)

    - Commotion Wireless – FOSS mesh networking
    - DD-WRT – Based on OpenWrt code, paid and free versions available
    - Gargoyle – A free OpenWrt-based Linux distribution for a range of Broadcom and Atheros chipset based wireless routers
    - LEDE – A fork of the OpenWrt project that shares many of the same goals
    - libreCMC – An FSF-endorsed derivation of OpenWRT with the proprietary blobs removed
    - Roofnet – A wireless community network project
    - ROOter – OpenWrt-based distribution aiming to convert a cheap router into one that supports 3G and 4G modems plus provide access to the modem to display signal and cell tower information

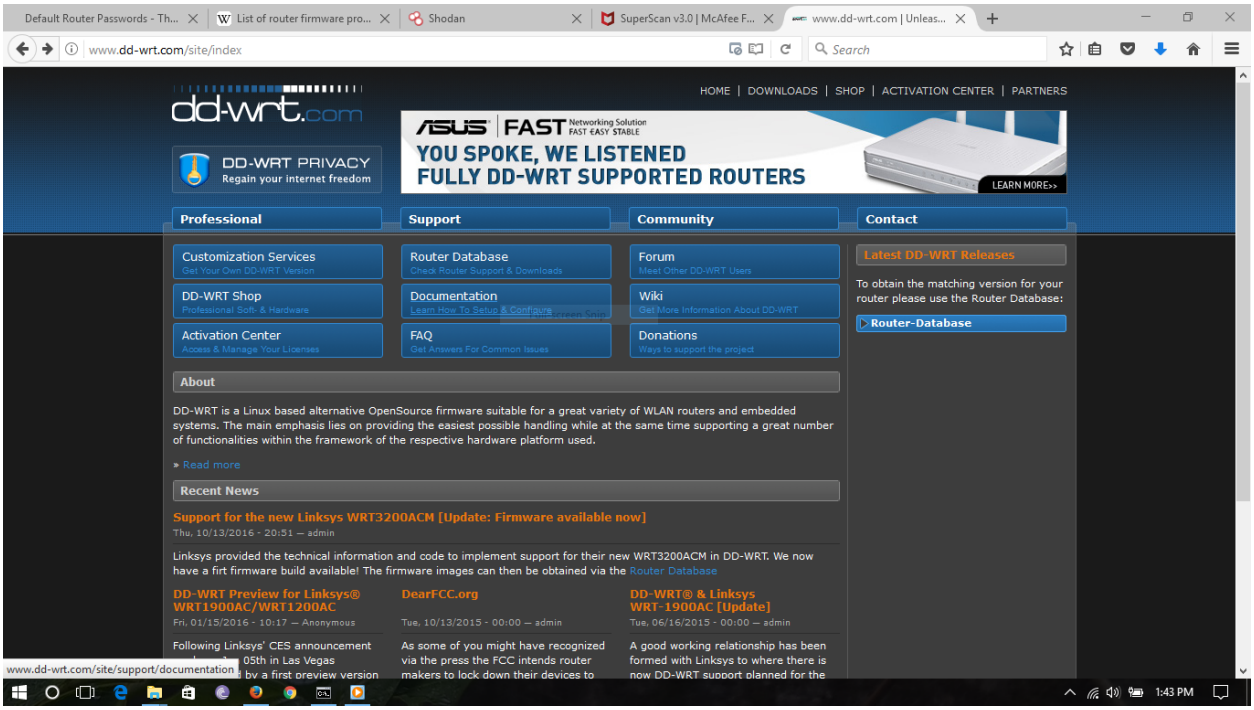
2. DebWRT – Combines the Linux kernel from OpenWrt and the package management system from Debian (Linux/GPL)

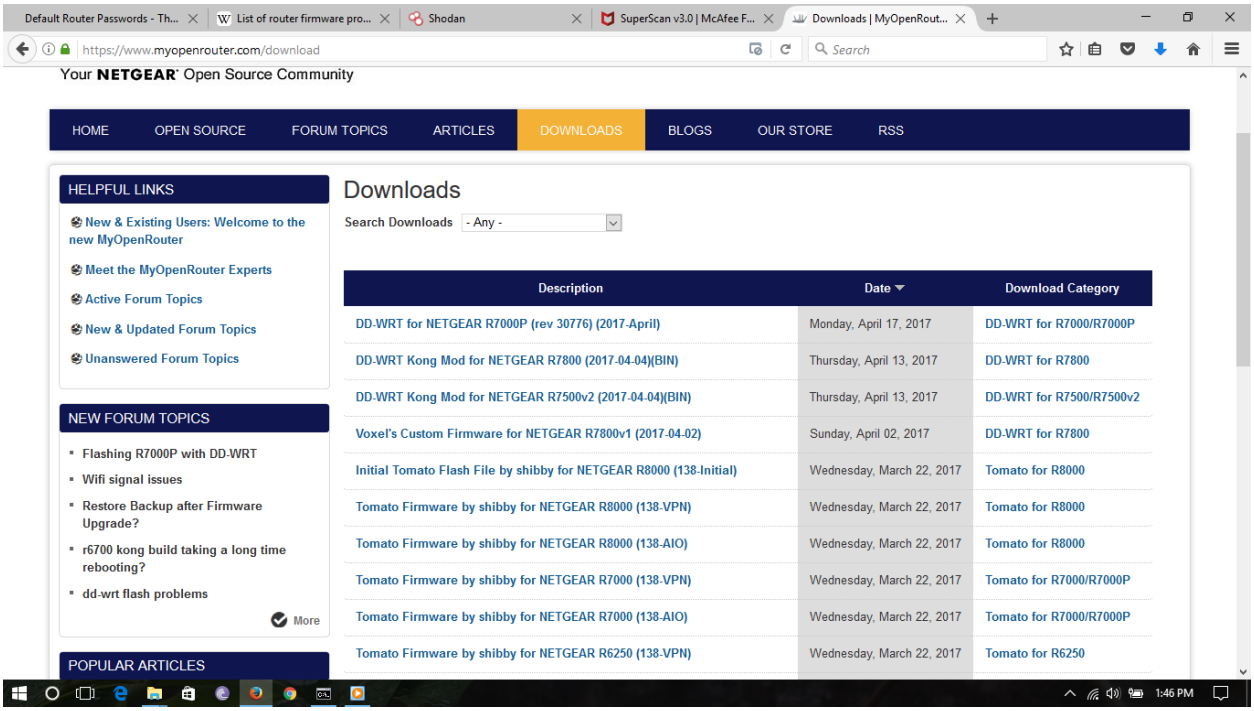
3. HyperWRT – Early power-boosting firmware project to stay close to the official WRT54G and WRT54GS firmware but add features such as transmit power, port triggers, scripts, telnet, etc.
    - Tomato – The successor to HyperWRT, features advanced QoS as well as Ajax and SVG graphs

4. Zeroshell – Routers and bridges with VPN, QoS, load balancing and other functionalities

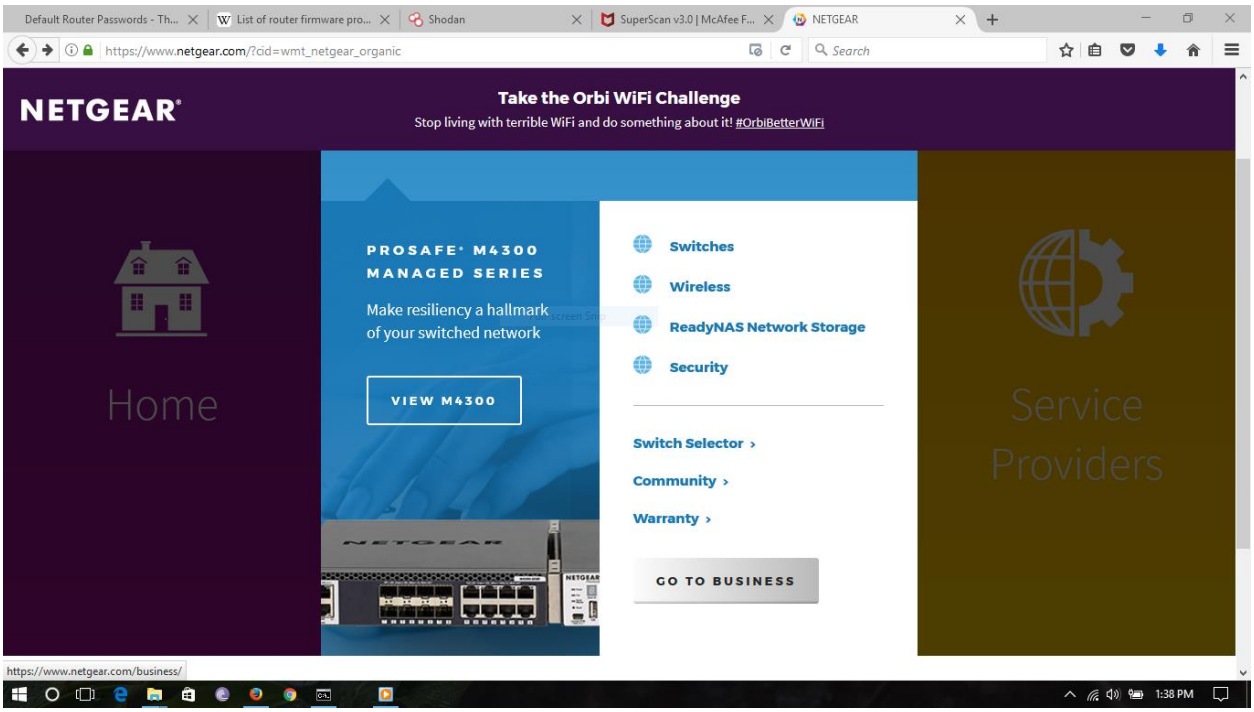
5. FreeBSD - A free Open source operating system (BSD licenses)
    - zrouter – a router fimware based on FreeBSD
    - BSD Router Project - BSD Router project based on FreeBSD that includes Quagga and Bird.
    - m0n0wall - m0n0wall is built on FreeBSD and boots off of a Compact Flash or CD ROM media in under 12 MB.
    - pfsense - an open source firewall/router computer software distribution based on FreeBSD that can be installed on a physical computer or a virtual machine

DD-wrt

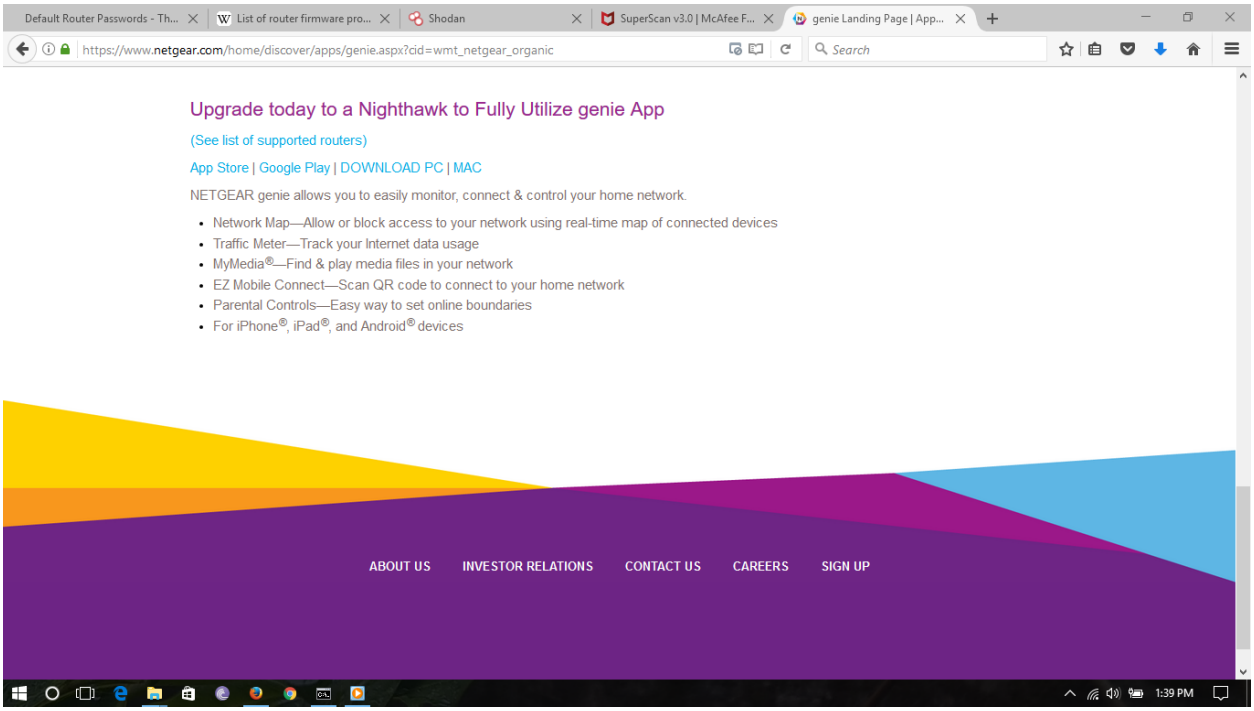




Myopenrouter

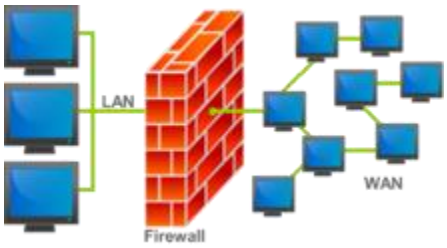


Netgear


Default Router Passwords - Th...
List of router firmware pro...
Shodan
SuperScan v3.0 | McAfee F...
genie Landing Page | App...
https://www.netgear.com/home/discover/apps/genie.aspx?cid=wmt_netgear_organic
Search
Upgrade today to a Nighthawk to Fully Utilize genie App
(See list of supported routers)
App Store | Google Play | DOWNLOAD PC | MAC
NETGEAR genie allows you to easily monitor, connect & control your home network.
Network Map—Allow or block access to your network using real-time map of connected devices
Traffic Meter—Track your Internet data usage
MyMedia®—Find & play media files in your network
EZ Mobile Connect—Scan QR code to connect to your home network
Parental Controls—Easy way to set online boundaries
For iPhone®, iPad®, and Android® devices
ABOUT US
INVESTOR RELATIONS
CONTACT US
CAREERS
SIGN UP
1:39 PM

Firewalls

In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware-based firewall computer appliances. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP or VPN server for that network.



Types

Firewalls are generally categorized as network-based or host-based. Network-based firewalls are positioned on the gateway computers of LANs, WANs and intranets. Host-based firewalls are positioned on the network node itself. The host-based firewall may be a daemon or service as a part of the operating system or an agent application such as endpoint security or protection. Each has advantages and disadvantages. However, each has a role in layered security.

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. The term "packet filter" originated in the context of BSD operating systems.

Network layer or packet filters

Network layer firewalls generally fall into two sub-categories, stateful and stateless. Stateful firewalls maintain context about active sessions, and use that "state information" to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, it will be evaluated according to the ruleset for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing.

Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or port, destination service like HTTP or FTP. They can filter based on protocols, TTL values, network block of the originator, of the source, and many other attributes.

Application-layer

Commonly used packet filters on various versions of Unix are ipfw (FreeBSD, Mac OS X (< 10.7)), NPF (NetBSD), PF (Mac OS X (> 10.4), OpenBSD, and some other BSDs), iptables/ipchains (Linux) and IPFilter.

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or FTP traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender).

On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and Trojans. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

Application firewalls function by determining whether a process should accept any given connection. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. Application firewalls that hook into socket calls are also referred to as socket filters. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter.

Also, application firewalls further filter connections by examining the process ID of data packets against a rule set for the local process involved in the data transmission. The extent of the filtering that occurs is defined by the provided rule set. Given the variety of software that exists, application firewalls only have more complex rule sets for the standard services, such as sharing services. These per-process rule sets have limited efficacy in filtering every possible association that may occur with other processes. Also, these per-process rule sets cannot defend against modification of the process via exploitation, such as memory corruption exploits. Because of these limitations, application firewalls are beginning to be supplanted by a new generation of application firewalls that rely on mandatory access control (MAC), also referred to as sandboxing, to protect vulnerable services.

Firewall	License	Cost and usage limits	OS
Avast Internet Security	Proprietary	US$39.99 per year	Microsoft Windows
Comodo Internet Security	Proprietary	Free	Windows 10/8.1/8/7/Vista x32/x64, XPx32
GlassWire	Proprietary	Free	Windows 7 / Windows 8 / Windows 10
Intego VirusBarrier	Proprietary	pay	Mac OS X 10.5 or later; on an Xserve
Kaspersky Internet Security	Proprietary	$59,95 Year / 30 day trial	Windows unknown versions x32/x64
Lavasoft Personal Firewall	Proprietary	€36 Year	Windows unknown versions x32/x64
Microsoft Forefront Threat Management Gateway	Proprietary	discontinued	Windows unknown versions x64
Norton 360	Proprietary	$59.99 Year	Windows unknown versions x32/x64
Online Armor Personal Firewall	Proprietary	discontinued	Windows unknown versions x32/x64
Outpost Firewall Pro	Proprietary	discontinued	Windows 10, 8, 7, Vista, XP x32/x64
PC Tools Firewall Plus	Proprietary	discontinued	Windows unknown versions x32/x64
Sygate Personal Firewall	Proprietary	discontinued	Windows unknown versions x32
Windows Firewall	Proprietary	Included with Windows XP SP2 and later	ALL Windows Versions x32/x64
ZoneAlarm	Proprietary	Free / Paid	Windows 7 / Vista / XP SP3/ Windows 8, 8.1. 10 x32/x64
Netfilter/iptables	GPL	Free	Linux kernel module

Firewall	License	Cost and usage limits	OS
nftables	GPL	Free	Linux kernel (>=3.13) module
Shorewall	GPL	Free	Linux-based appliance
PeerBlock	GPL	Free	Windows 8/8.1, 7, Vista x32/64
NPF	BSD	Free	NetBSD kernel module
PF	BSD	Free	*BSD kernel module
ipfirewall	BSD	Free	*BSD package
IPFilter	GPLv2	Free	Package for multiple UNIX-like operating systems

Filtering features

Can Target:	Changing default policy to accept/reject (by issuing a single rule)	IP destination address(es)	IP source address(es)	TCP/UDP destination port(s)	TCP/UDP source port(s)	Ethernet MAC destination address	Ethernet MAC source address	Inbound firewall (ingress)	Outbound firewall (egress)
IPFire	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Trend Micro Internet Security	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Untangle	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Vyatta	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Windows XP Firewall	No	No	Yes	Partial	No	No	No	Yes	No
Windows Vista Firewall	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Windows 7 / Windows 2008 R2 Firewall	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
WinGate	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes
Zeroshell	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Zorp	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
pfSense	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Dynamic Packet Filtering

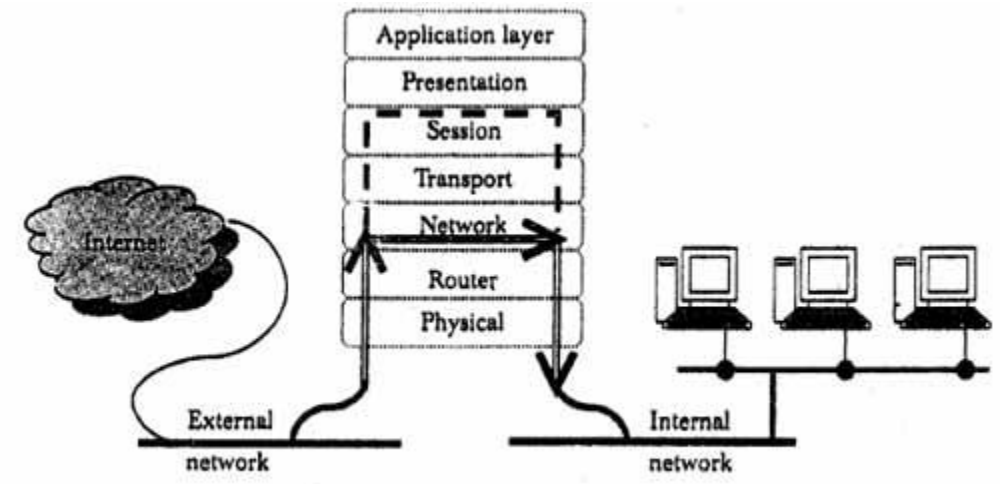
Dynamic packet filtering is a firewall and routing capability that provides network packet filtering based not only on packet information in the current packet, but also on previous packets that have been sent. For example without dynamic packet filtering, a connection response may be allowed to go from the internet to the secure part of the network. Dynamic packet filtering would consider whether a connection was started from inside the secure part of the network and only allow a connection response from the internet if the packet appeared to be a response to the request.

Dynamic packet filtering filters packets based on:

- Administrator defined rules governing allowed ports and IP addresses at the network and transport layers of the OSI network model.
- Connection state which considers prior packets that have gone through the firewall.
- Packet contents including the application layer contents

Static packet filtering only filters packets based on administrator defined rules governing allowed ports and IP addresses at the network and transport layers of the OSI network model as mentioned in item 1 above. Therefore dynamic packet filtering also called stateful inspection provides additional capabilities including inspection of packet contents up to the application layer and consideration of the state of any connections.

Dynamic packet filtering provides a better level of security than static packet filtering since it takes a closer look at the contents of the packet and also considers previous connection states.



Dynamic packet filter

Virtual firewall

A virtual firewall (VF) is a network firewall service or appliance running entirely within a virtualized environment and which provides the usual packet filtering and monitoring provided via a physical network firewall. The VF can be realized as a traditional software firewall on a guest virtual machine already running, a purpose-built virtual security appliance designed with virtual network security in mind, a virtual switch with additional security capabilities, or a managed kernel process running within the host hypervisor.

One method to secure, log and monitor VM-to-VM traffic involved routing the virtualized network traffic out of the virtual network and onto the physical network via VLANs, and hence into a physical firewall already present to provide security and compliance services for the physical network. The VLAN traffic could be monitored and filtered by the physical firewall and then passed back into the virtual network (if deemed legitimate for that purpose) and on to the target virtual machine.

Not surprisingly, LAN managers, security experts and network security vendors began to wonder if it might be more efficient to keep the traffic entirely within the virtualized environment and secure it from there.

A virtual firewall then is a firewall service or appliance running entirely within a virtualised environment — even as another virtual machine, but just as readily within the hypervisor itself — providing the usual packet filtering and monitoring that a physical firewall provides. The VF can be installed as a traditional software firewall on a guest VM already running within the virtualized environment; or it can be a purpose-built virtual security appliance designed with virtual network security in mind; or it can be a virtual switch with additional security capabilities; or it can be a managed kernel process running within the host hypervisor that sits atop all VM activity.

The current direction in virtual firewall technology is a combination of security-capable virtual switches, and virtual security appliances. Some virtual firewalls integrate additional networking functions such as site-to-site and remote access VPN, QoS, URL filtering and more.

Virtual firewalls can operate in different modes to provide security services, depending on the point of deployment. Typically these are either bridge-mode or hypervisor-mode (hypervisor-based, hypervisor-resident). Both may come shrink wrapped as a virtual security appliance and may install a virtual machine for management purposes.

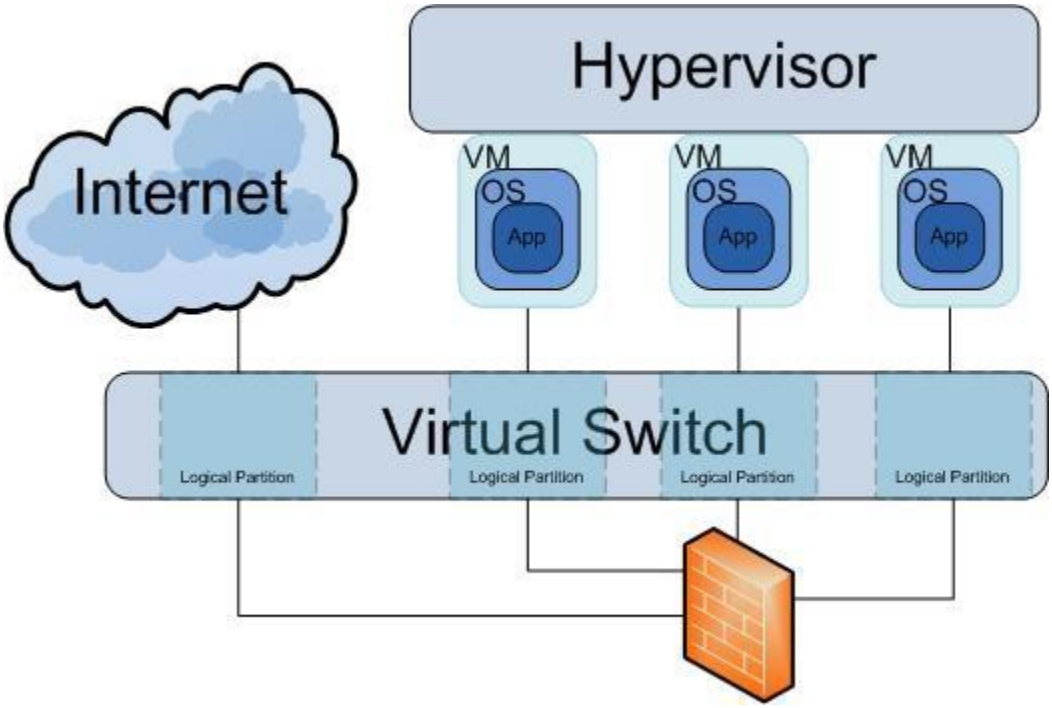
A virtual firewall operating in bridge-mode acts like its physical-world firewall analog; it sits in a strategic part of the network infrastructure — usually at an inter-network virtual switch or bridge — and intercepts network traffic destined for other network segments and needing to travel over the bridge. By examining the source origin, the destination, the type of packet it is and even the payload the VF can decide if the packet is to be allowed passage, dropped, rejected, or forwarded or mirrored to some other device. Initial entrants into the virtual firewall field were largely bridge-mode, and many offers retain this feature.

By contrast, a virtual firewall operating in hypervisor-mode is not actually part of the virtual network at all, and as such has no physical-world device analog. A hypervisor-mode virtual firewall resides in the

virtual machine monitor or hypervisor where it is well positioned to capture VM activity including packet injections. The entire monitored VM and all its virtual hardware, software, services, memory and storage can be examined, as can changes in these. Further, since a hypervisor-based virtual firewall is not part of the network proper and is not a virtual machine its functionality cannot be monitored in turn or altered by users and software limited to running under a VM or having access only to the virtualized network.

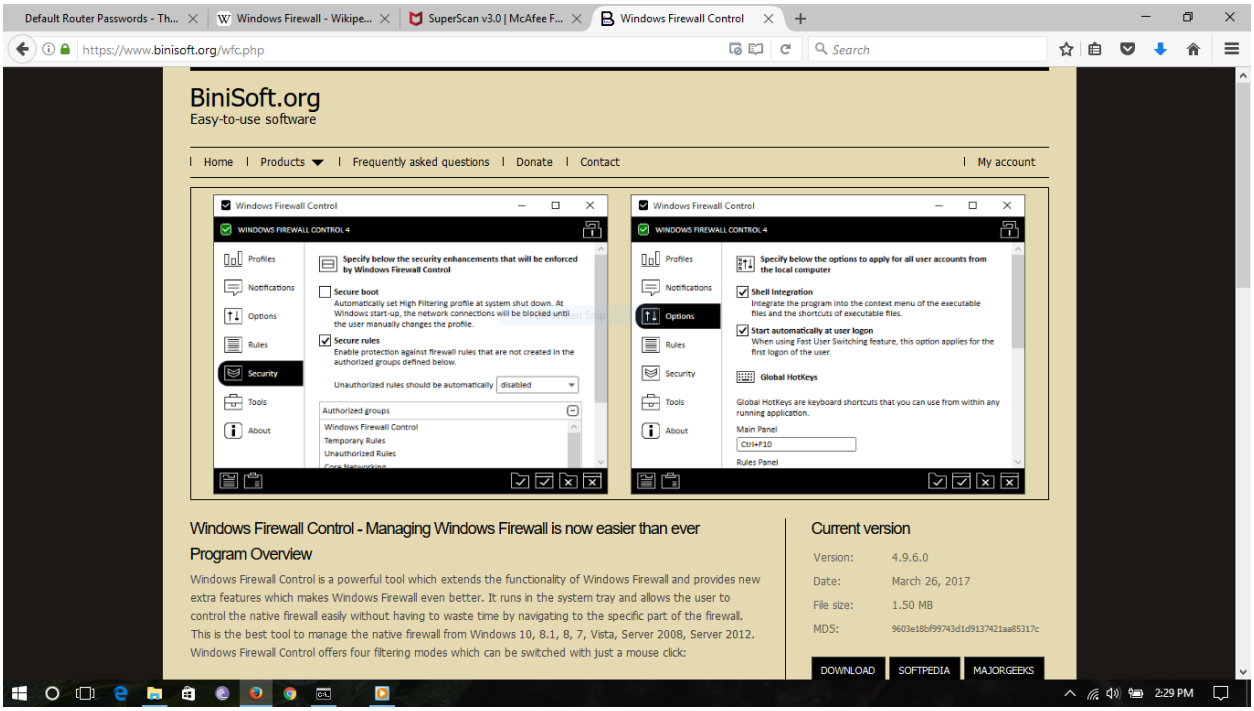
Bridge-mode virtual firewalls can be installed just as any other virtual machine in the virtualized infrastructure. Since it is then a virtual machine itself, the relationship of the VF to all the other VM may become complicated over time due to VMs disappearing and appearing in random ways, migrating between different physical hosts, or other uncoordinated changes allowed by the virtualized infrastructure.

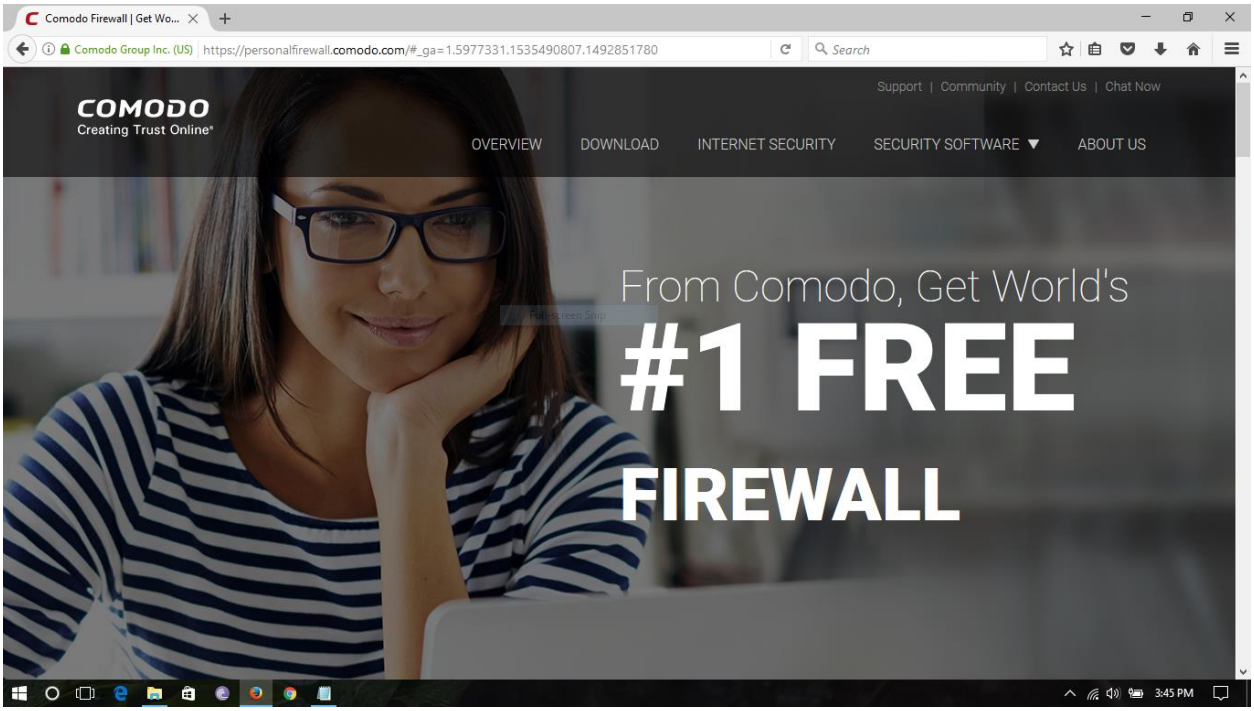
Hypervisor-mode virtual firewalls require a modification to the physical host hypervisor kernel in order to install process hooks or modules allowing the virtual firewall system access to VM information and direct access to the virtual network switches and virtualized network interfaces moving packet traffic between VMs or between VMs and the network gateway. The hypervisor-resident virtual firewall can use the same hooks to then perform all the customary firewall functions like packet inspection, dropping, and forwarding but without actually touching the virtual network at any point. Hypervisor-mode virtual firewalls can be very much faster than the same technology running in bridge-mode because they are not doing packet inspection in a virtual machine, but rather from within the kernel at native hardware speeds.



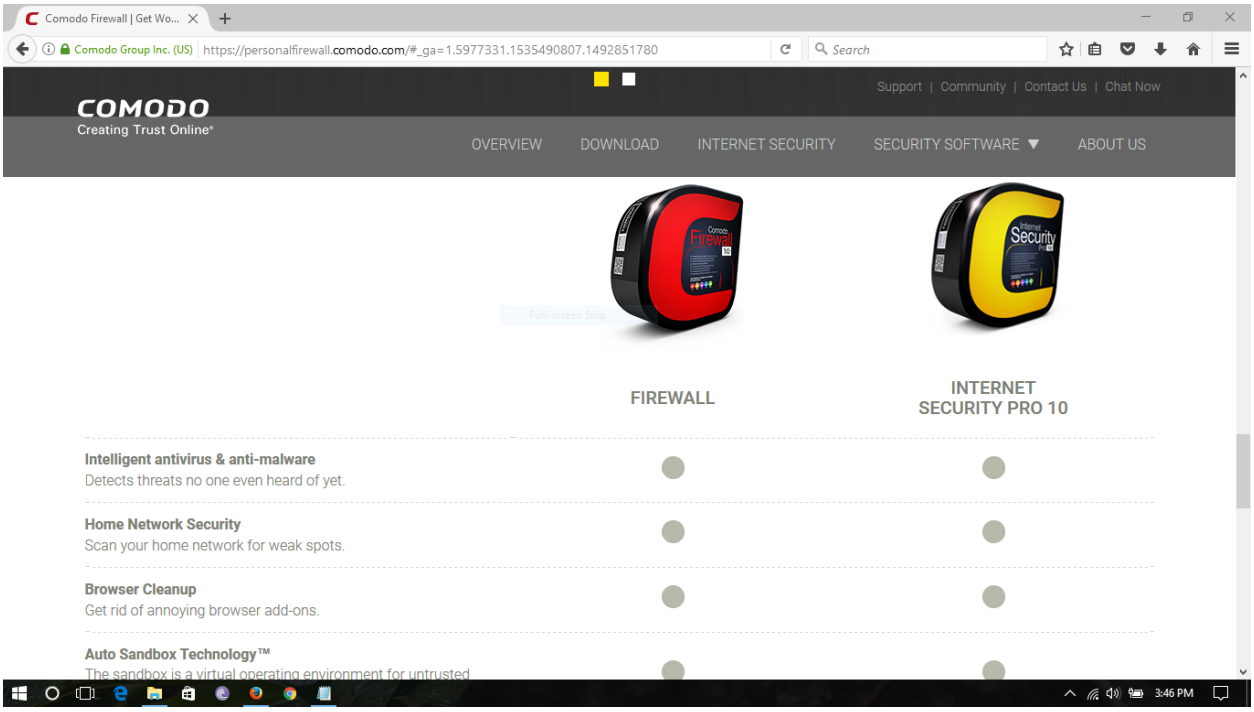
Host Based Firewalls:

Binisoft.org

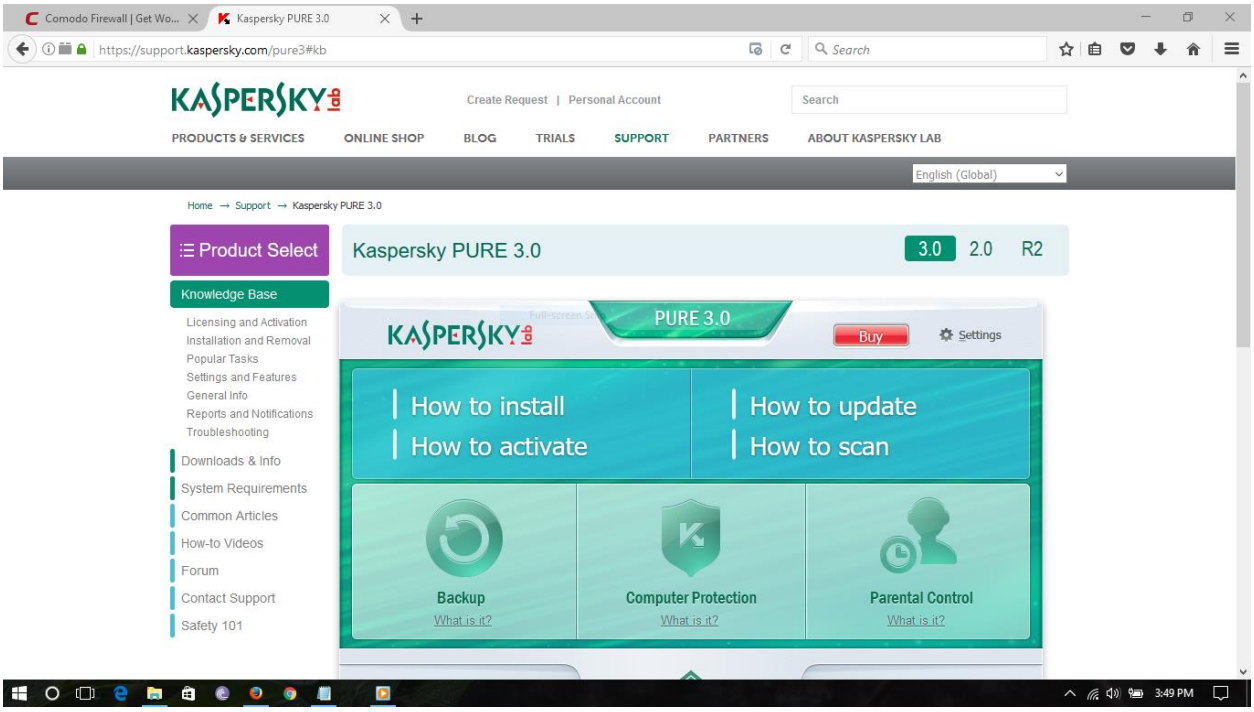




Comodo


Comodo Firewall | Get Wo...
Comodo Group Inc. (US)
https://personalfirewall.comodo.com/#_ga=1.5977331.1535490807.1492851780
Search
COMODO
Creating Trust Online®
Support | Community | Contact Us | Chat Now
OVERVIEW
DOWNLOAD
INTERNET SECURITY
SECURITY SOFTWARE
ABOUT US
FIREWALL
INTERNET SECURITY PRO 10
Intelligent antivirus & anti-malware
Detects threats no one even heard of yet.
Home Network Security
Scan your home network for weak spots.
Browser Cleanup
Get rid of annoying browser add-ons.
Auto Sandbox Technology™
3:46 PM

Kaspersky


Comodo Firewall | Get Wo...
Kaspersky PURE 3.0
https://support.kaspersky.com/pure3#kb
Search
KASPERSKY lab
Create Request | Personal Account
Search
PRODUCTS & SERVICES
ONLINE SHOP
BLOG
TRIALS
SUPPORT
PARTNERS
ABOUT KASPERSKY LAB
English (Global)
Home → Support → Kaspersky PURE 3.0
Product Select
Kaspersky PURE 3.0
3.0
2.0
R2
Knowledge Base
Licensing and Activation
Installation and Removal
Popular Tasks
Settings and Features
General Info
Reports and Notifications
Troubleshooting
Downloads & Info
System Requirements
Common Articles
How-to Videos
Forum
Contact Support
Safety 101
PURE 3.0
Buy
Settings
How to install
How to activate
How to update
How to scan
Backup
What is it?
Computer Protection
What is it?
Parental Control
What is it?
3:49 PM

Network based

Firewall configuration

Global firewall settings:

Name	Type	Required	Default	Description
input	string	no	REJECT	Set policy for the INPUT chain of the filter table.
output	string	no	REJECT	Set policy for the OUTPUT chain of the filter table.
forward	string	no	REJECT	Set policy for the FORWARD chain of the filter table.
drop_invalid	boolean	no	0	Drop invalid packets (e.g. not matching any active connection).
syn_flood	boolean	no	0	Enable SYN flood protection (obsoleted by synflood_protect setting).
synflood_protect	boolean	no	0	Enable SYN flood protection.
synflood_rate	string	no	25	Set rate limit (packets/second) for SYN packets above which the traffic is considered a flood.
synflood_burst	string	no	50	Set burst limit for SYN packets above which the traffic is considered a flood if it exceeds the allowed rate.
tcp_syncookies	boolean	no	1	Enable the use of SYN cookies.
tcp_ecn	boolean	no	0	
tcp_westwood	boolean	no	0	
tcp_window_scaling	boolean	no	1	Enable TCP window scaling.
accept_redirects	boolean	no	0	
accept_source_route	boolean	no	0	

Name	Type	Required	Default	Description
custom_chains	boolean	no	1	
disable_ipv6	boolean	no	0	Disable IPv6 firewall rules.

Redirects

Name	Type	Required	Default	Description
src	zone name	yes for DNAT target	*(none)*	Specifies the traffic *source zone*. Must refer to one of the defined *zone names*. For typical port forwards this usually is wan
src_ip	ip address	no	*(none)*	Match incoming traffic from the specified *source ip address*
src_dip	ip address	yes for SNAT target	*(none)*	For *DNAT*, match incoming traffic directed at the given *destination ip address*. For *SNAT* rewrite the *source address* to the given address.
src_mac	mac address	no	*(none)*	Match incoming traffic from the specified *mac address*
src_port	port or range	no	*(none)*	Match incoming traffic originating from the given *source port or port range (ex: '5000-5100')* on the client host
src_dport	port or range	no	*(none)*	For *DNAT*, match incoming traffic directed at the given *destination port or port range (ex: '5000-5100')* on this host. For *SNAT* rewrite the *source ports* to the given value.
proto	protocol name or number	yes	*tcpudp*	Match incoming traffic using the given *protocol*
dest	zone name	yes for SNAT target	*(none)*	Specifies the traffic *destination zone*. Must refer to one of the defined *zone names*. For DNAT target on Attitude Adjustment, NAT reflection works only if this is equal to lan.

Name	Type	Required	Default	Description
dest_ip	ip address	yes for DNAT target	*(none)*	For *DNAT*, redirect matched incoming traffic to the specified internal host. For *SNAT*, match traffic directed at the given address. For *DNAT* if the dest_ip value matches the local ip addresses of the router, as shown in the ifconfig, then the rule is translated in a DNAT + input 'accept' rule. Otherwise it is a DNAT + forward rule
dest_port	port or range	no	*(none)*	For *DNAT*, redirect matched incoming traffic to the given port on the internal host. For *SNAT*, match traffic directed at the given ports. Only a single port or range can be specified (ex: '5000-5100'), not disparate ports as with Rules (below)
ipset	string	no	*(none)*	If specified, match traffic against the given *ipset*. The match can be inverted by prefixing the value with an exclamation mark
mark	string	no	*(none)*	If specified, match traffic against the given firewall mark, e.g. 0xFF to match mark 255 or 0x0/0x1 to match any even mark value. The match can be inverted by prefixing the value with an exclamation mark, e.g. !0x10 to match all but mark #16.
start_date	date (yyyy-mm-dd)	no	*(always)*	If specifed, only match traffic after the given date (inclusive).
stop_date	date (yyyy-mm-dd)	no	*(always)*	If specified, only match traffic before the given date (inclusive).
start_time	time (hh:mm:ss)	no	*(always)*	If specified, only match traffic after the given time of day (inclusive).
stop_time	time (hh:mm:ss)	no	*(always)*	If specified, only match traffic before the given time of day (inclusive).
weekdays	list of weekdays	no	*(always)*	If specified, only match traffic during the given week days, e.g. sun mon thu fri to only match on sundays, mondays, thursdays and fridays. The list can be inverted by

Name	Type	Required	Default	Description
				prefixing it with an exclamation mark, e.g. `! sat sun` to always match but on saturdays and sundays.
`monthdays`	list of dates	no	*(always)*	If specified, only match traffic during the given days of the month, e.g. `2 5 30` to only match on every 2nd, 5th and 30rd day of the month. The list can be inverted by prefixing it with an exclamation mark, e.g. `! 31` to always match but on the 31st of the month.
`utc_time`	boolean	no	`0`	Treat all given time values as UTC time instead of local time.
`target`	string	no	`DNAT`	NAT target (`DNAT` or `SNAT`) to use when generating the rule
`family`	string	no	`any`	Protocol family (`ipv4`, `ipv6` or `any`) to generate iptables rules for.
`reflection`	boolean	no	`1`	Activate NAT reflection for this redirect - applicable to `DNAT` targets.
`reflection_src`	string	no	`internal`	The source address to use for NAT-reflected packets if `reflection` is `1`. This can be `internal` or `external`, specifying which interface's address to use. Applicable to `DNAT` targets.
`limit`	string	no	*(none)*	Maximum average matching rate; specified as a number, with an optional `/second`, `/minute`, `/hour` or `/day` suffix. Examples: `3/second`, `3/sec` or `3/s`.
`limit_burst`	integer	no	`5`	Maximum initial number of packets to match, allowing a short-term average above `limit`
`extra`	string	no	*(none)*	Extra arguments to pass to iptables. Useful mainly to specify additional match options, such as `-m policy --dir in` for IPsec.
`enabled`	string	no	`1` or `yes`	Enable the redirect rule or not.

Opening ports

```
config rule
        option src              wan
        option dest_port        22
        option target           ACCEPT
        option proto            tcp
```

Opening ports for selected subnet/host

```
config rule
        option src              wan
        option src_ip           '12.34.56.64/28'
        option dest_port        22
        option target           ACCEPT
        option proto            tcp
```

Port forwarding for IPv4 (Destination NAT/DNAT)

```
config redirect
        option src       wan
        option src_dport 80
        option proto     tcp
        option dest      lan
        option dest_ip   192.168.1.10
```

Transparent proxy rule (same host)

```
config redirect
        option src              lan
        option proto            tcp
        option src_dport        80
        option dest_port        3128
        option dest_ip          192.168.1.1
```

Transparent proxy rule (external)

```
config redirect
        option src              lan
        option proto            tcp
        option src_ip           !192.168.1.100
        option src_dport        80
        option dest_ip          192.168.1.100
        option dest_port        3128
        option target           DNAT

config redirect
        option dest             lan
        option proto            tcp
        option src_dip          192.168.1.1
        option dest_ip          192.168.1.100
        option dest_port        3128
        option target           SNAT
```

IPSec passthrough

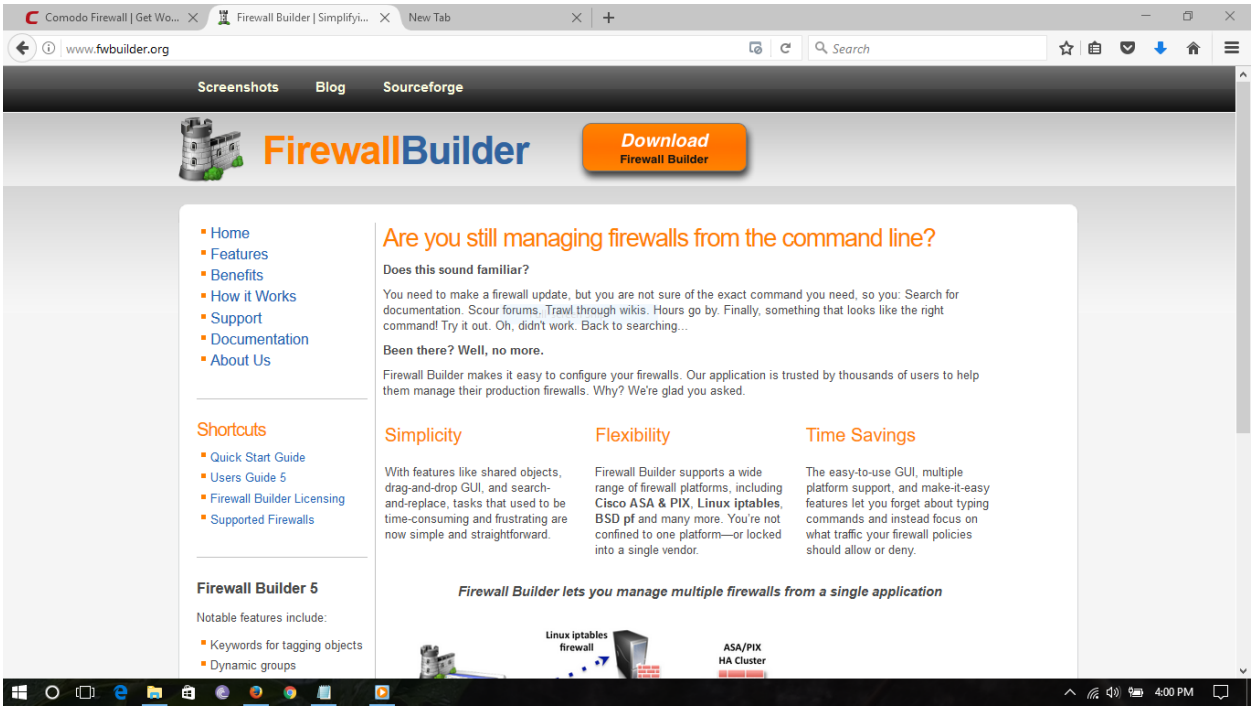
```
# AH protocol
config rule
        option src              wan
        option dest             lan
        option proto            ah
        option target           ACCEPT

# ESP protocol
config rule
        option src              wan
        option dest             lan
        option proto            esp
        option target           ACCEPT


# ISAKMP protocol
config rule
        option src              wan
        option dest             lan
        option proto            udp
        option src_port         500
        option dest_port        500
        option target           ACCEPT
```

Forwarding IPv6 tunnel traffic

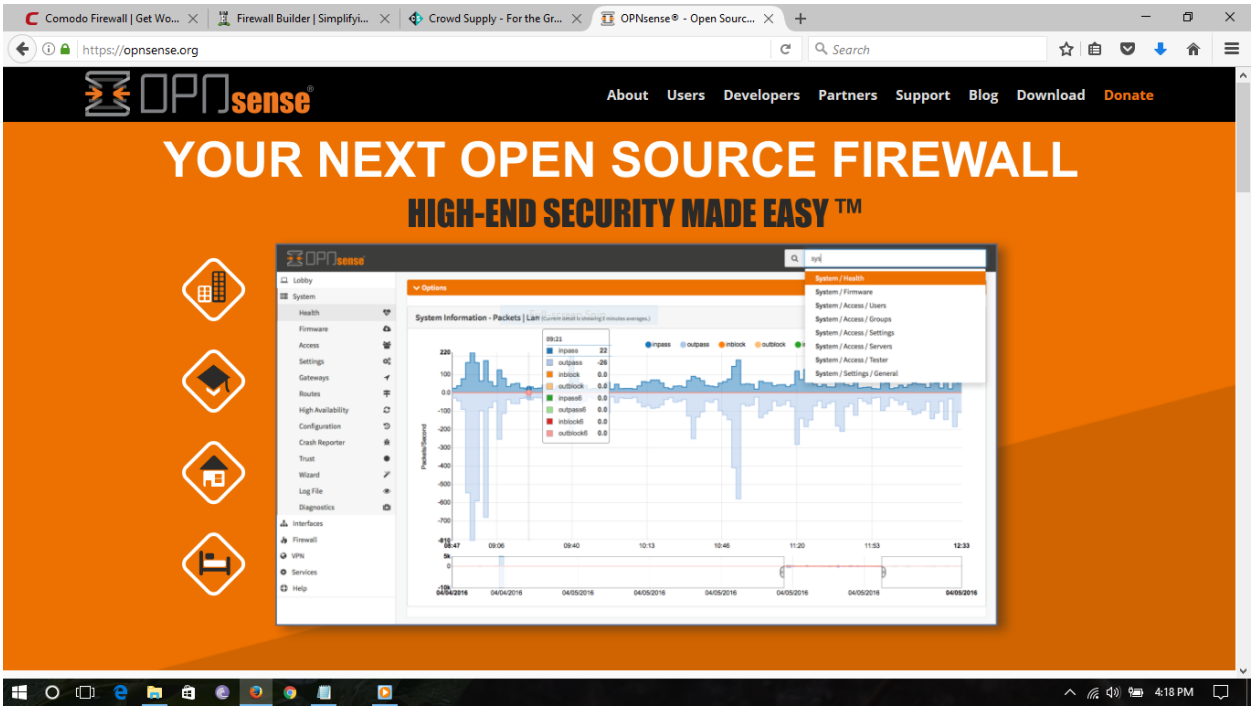
```
config zone
        option name wan6
        option network henet
        option family ipv6
        option input ACCEPT
        option output ACCEPT
        option forward REJECT

config forwarding
        option dest lan
        option src wan6
#you don't need the below as you can a firewall rule to open the port that
you need
config forwarding
        option dest wan6
        option src lan
```

Network Based firewalls:

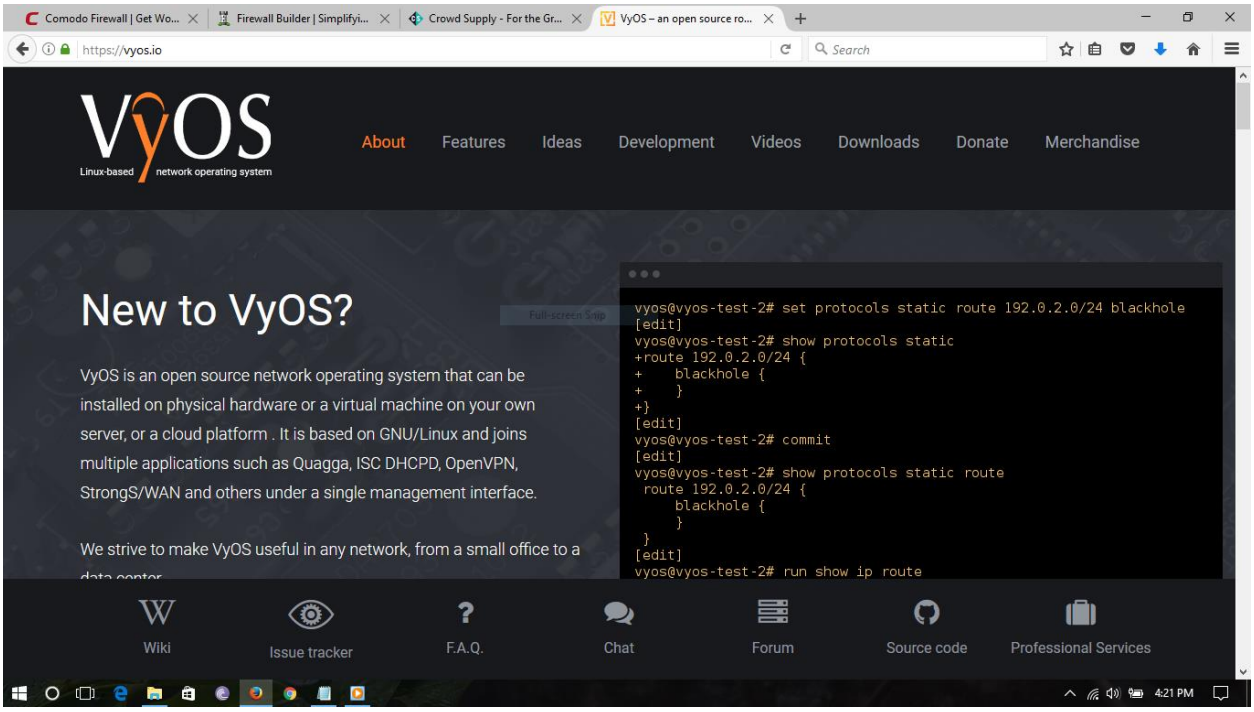
FirewallBuilder



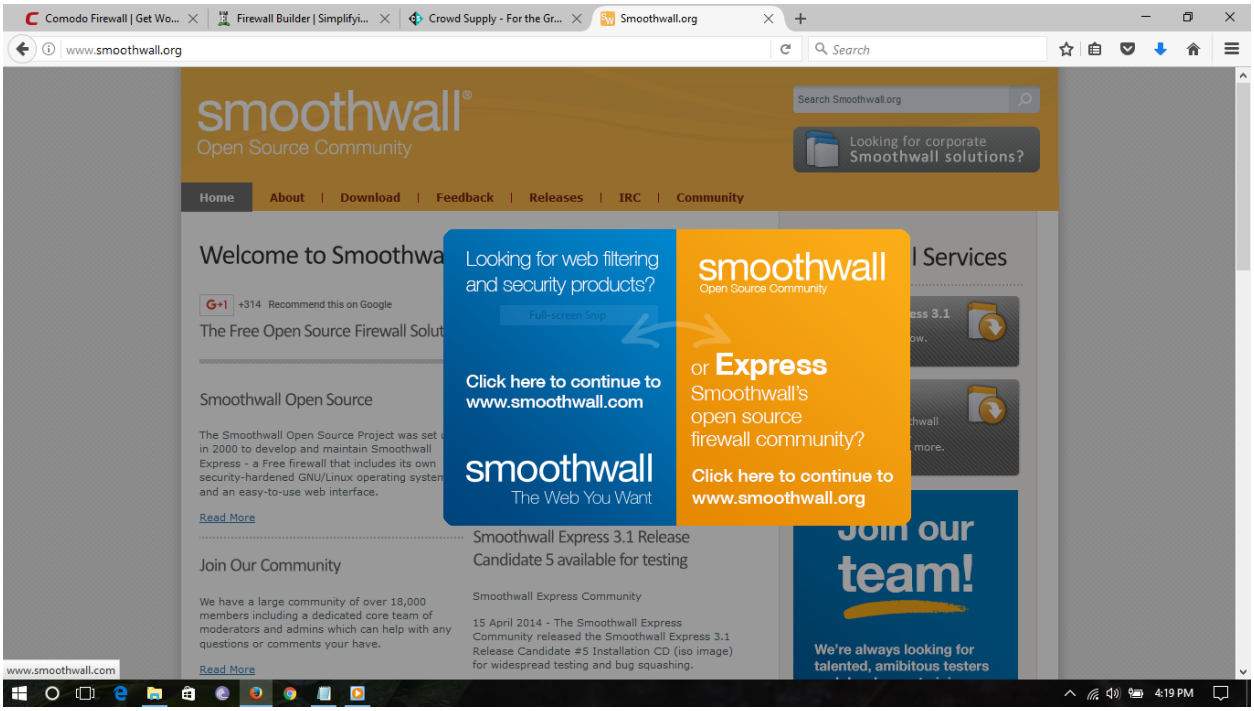
Opensense



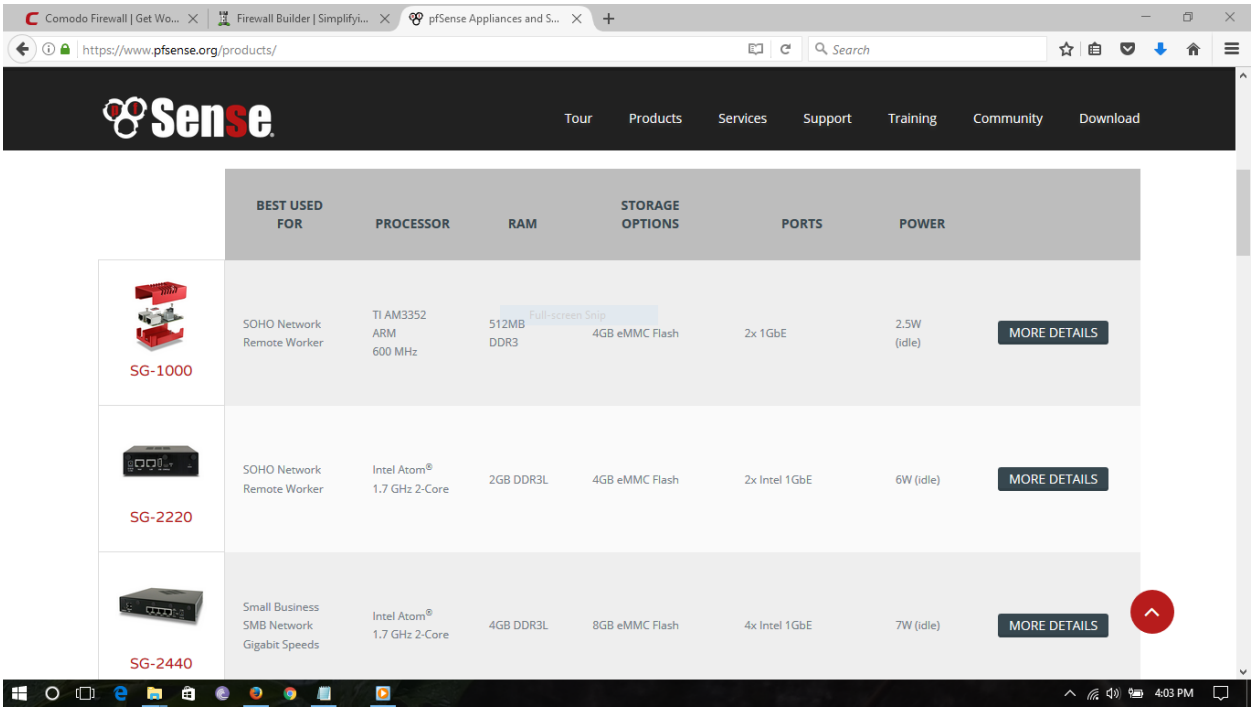
Vyos

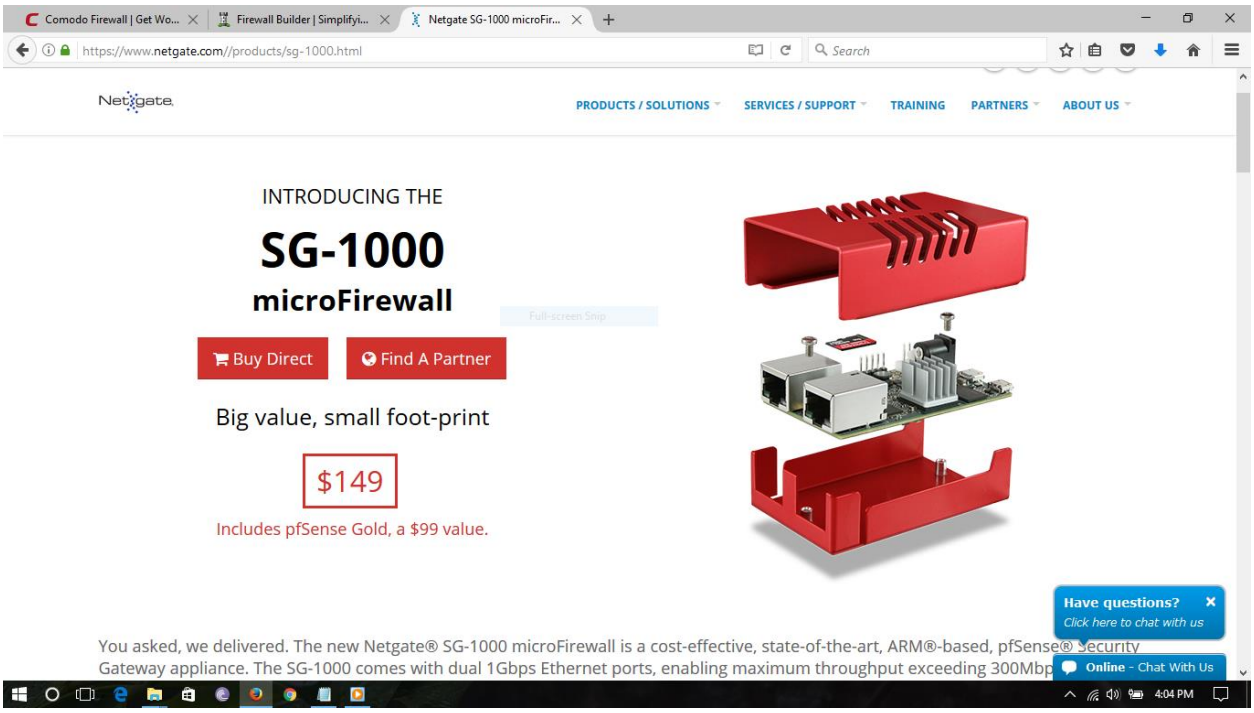


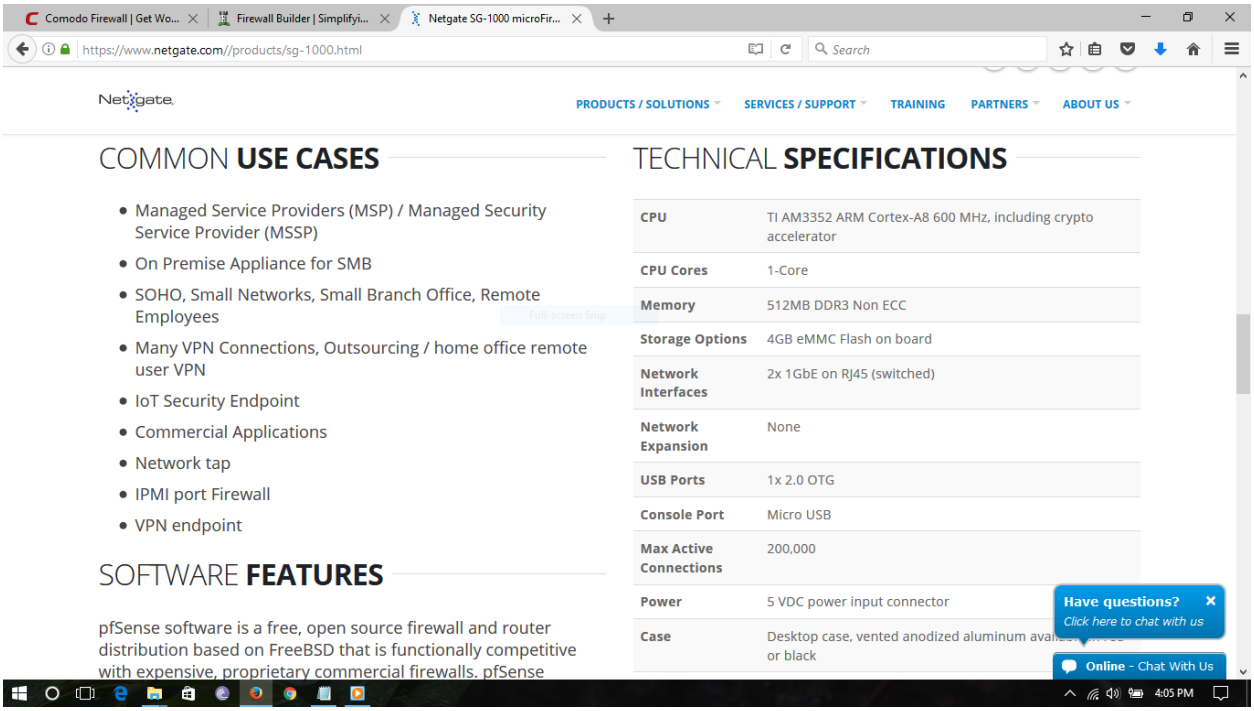
Smoothwall



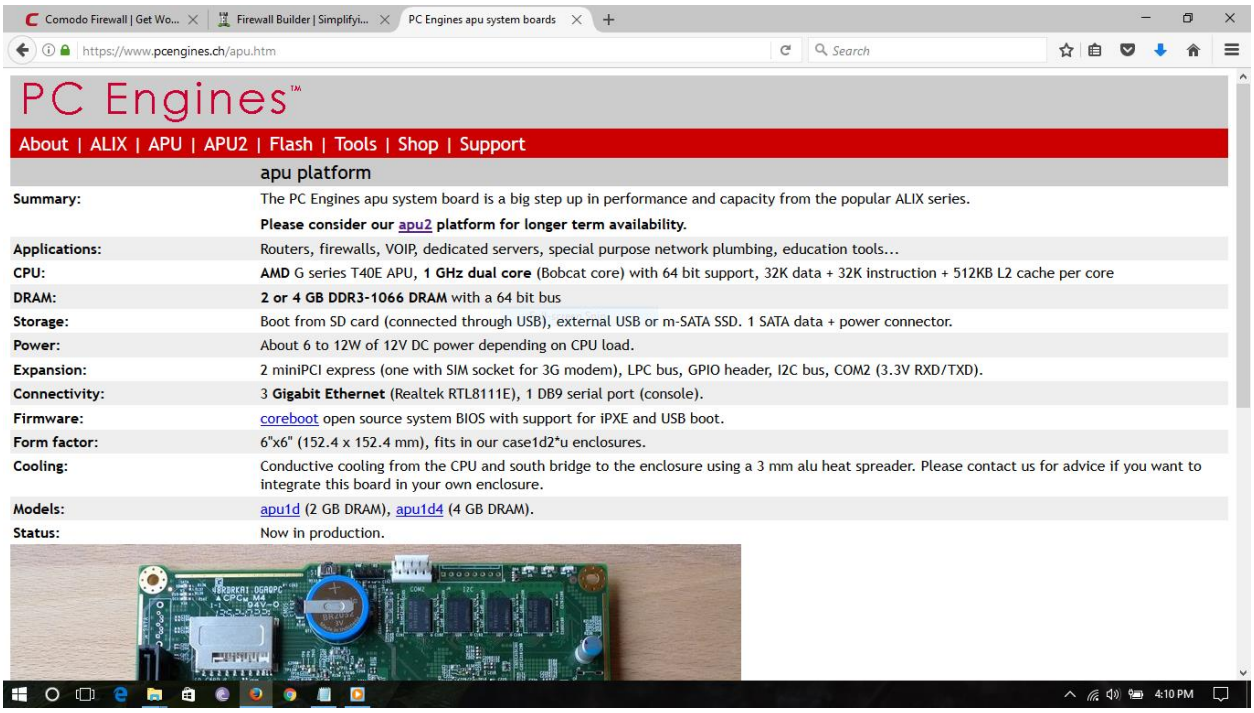
Pfsense

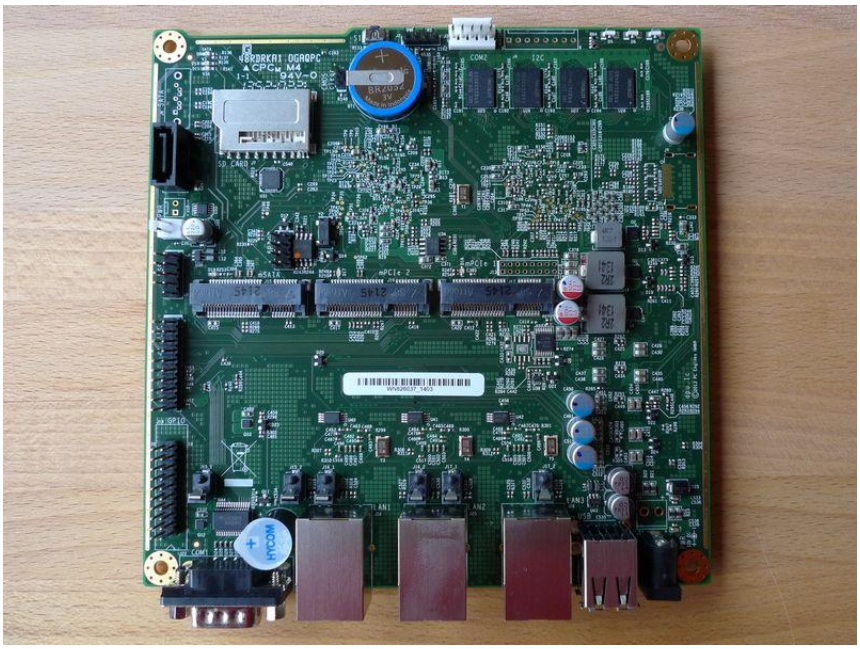

Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
pfSense Appliances and S...
https://www.pfsense.org/products/
Search
Sense
Tour
Products
Services
Support
Training
Community
Download
BEST USED FOR
PROCESSOR
RAM
STORAGE OPTIONS
PORTS
POWER
SG-1000
SOHO Network
Remote Worker
TI AM3352
ARM
600 MHz
512MB
DDR3
4GB eMMC Flash
2x 1GbE
2.5W
(idle)
MORE DETAILS
SG-2220
SOHO Network
Remote Worker
Intel Atom®
1.7 GHz 2-Core
2GB DDR3L
4GB eMMC Flash
2x Intel 1GbE
6W (idle)
MORE DETAILS
SG-2440
Small Business
SMB Network
Gigabit Speeds
Intel Atom®
1.7 GHz 2-Core
4GB DDR3L
8GB eMMC Flash
4x Intel 1GbE
7W (idle)
MORE DETAILS
4:03 PM


Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
Netgate SG-1000 microFir...
https://www.netgate.com//products/sg-1000.html
Search
Netgate
PRODUCTS / SOLUTIONS
SERVICES / SUPPORT
TRAINING
PARTNERS
ABOUT US
INTRODUCING THE
SG-1000
microFirewall
Buy Direct
Find A Partner
Big value, small foot-print
$149
Includes pfSense Gold, a $99 value.
Have questions?
Click here to chat with us
Online - Chat With Us
You asked, we delivered. The new Netgate® SG-1000 microFirewall is a cost-effective, state-of-the-art, ARM®-based, pfSense® Security
Gateway appliance. The SG-1000 comes with dual 1Gbps Ethernet ports, enabling maximum throughput exceeding 300Mbp
4:04 PM


Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
Netgate SG-1000 microFir...
https://www.netgate.com//products/sg-1000.html
Search
Netgate
PRODUCTS / SOLUTIONS
SERVICES / SUPPORT
TRAINING
PARTNERS
ABOUT US
COMMON USE CASES
Managed Service Providers (MSP) / Managed Security Service Provider (MSSP)
On Premise Appliance for SMB
SOHO, Small Networks, Small Branch Office, Remote Employees
Many VPN Connections, Outsourcing / home office remote user VPN
IoT Security Endpoint
Commercial Applications
Network tap
IPMI port Firewall
VPN endpoint
SOFTWARE FEATURES
pfSense software is a free, open source firewall and router distribution based on FreeBSD that is functionally competitive with expensive, proprietary commercial firewalls. pfSense
TECHNICAL SPECIFICATIONS
CPU
TI AM3352 ARM Cortex-A8 600 MHz, including crypto accelerator
CPU Cores
1-Core
Memory
512MB DDR3 Non ECC
Storage Options
4GB eMMC Flash on board
Network Interfaces
2x 1GbE on RJ45 (switched)
Network Expansion
None
USB Ports
1x 2.0 OTG
Console Port
Micro USB
Max Active Connections
200,000
Power
5 VDC power input connector
Case
Desktop case, vented anodized aluminum
or black
Have questions?
Click here to chat with us
Online - Chat With Us
4:05 PM

Apu


Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
PC Engines apu system boards
https://www.pcengines.ch/apu.htm
Search
PC Engines™
About | ALIX | APU | APU2 | Flash | Tools | Shop | Support
apu platform
Summary:
The PC Engines apu system board is a big step up in performance and capacity from the popular ALIX series.
Please consider our apu2 platform for longer term availability.
Applications:
Routers, firewalls, VOIP, dedicated servers, special purpose network plumbing, education tools...
CPU:
AMD G series T40E APU, 1 GHz dual core (Bobcat core) with 64 bit support, 32K data + 32K instruction + 512KB L2 cache per core
DRAM:
2 or 4 GB DDR3-1066 DRAM with a 64 bit bus
Storage:
Boot from SD card (connected through USB), external USB or m-SATA SSD. 1 SATA data + power connector.
Power:
About 6 to 12W of 12V DC power depending on CPU load.
Expansion:
2 miniPCI express (one with SIM socket for 3G modem), LPC bus, GPIO header, I2C bus, COM2 (3.3V RXD/TXD).
Connectivity:
3 Gigabit Ethernet (Realtek RTL8111E), 1 DB9 serial port (console).
Firmware:
coreboot open source system BIOS with support for iPXE and USB boot.
Form factor:
6"x6" (152.4 x 152.4 mm), fits in our case1d2*u enclosures.
Cooling:
Conductive cooling from the CPU and south bridge to the enclosure using a 3 mm alu heat spreader. Please contact us for advice if you want to integrate this board in your own enclosure.
Models:
apu1d (2 GB DRAM), apu1d4 (4 GB DRAM).
Status:
Now in production.
4:10 PM



Alix2d2

Comodo Firewall | Get Wo... | Firewall Builder | Simplifyi... | PC Engines alix2d2 product file

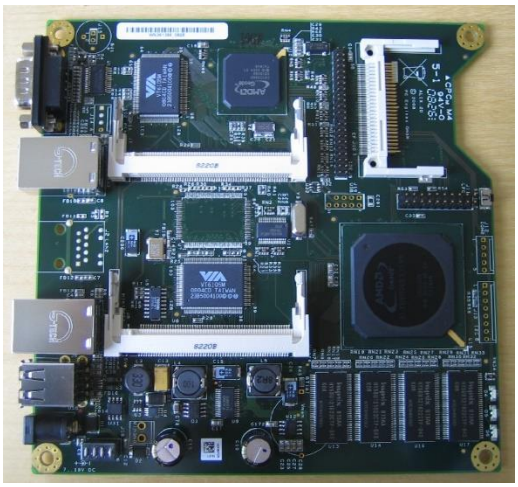
https://www.pcengines.ch/alix2d2.htm

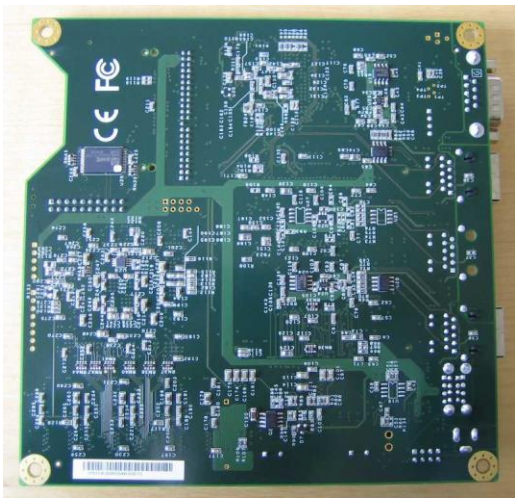
PC Engines™

About | ALIX | APU | APU2 | Flash | Tools | Shop | Support

alix2d2	System board
Status	Active, but not recommended for new designs.
Part numbers	**alix2d2** = 2 LAN / 2 miniPCI / LX800 / 256 MB / USB
Spec	• CPU: 500 MHz AMD Geode LX800 • DRAM: 256 MB DDR DRAM • Storage: CompactFlash socket, 44 pin IDE header • Power: DC jack or passive POE, min. 7V to max. 20V • Three front panel LEDs, pushbutton • Expansion: 2 miniPCI slots, LPC bus • Connectivity: 2 Ethernet channels (Via VT6105M 10/100) • I/O: DB9 serial port, dual USB port • Board size: 6 x 6" (152.4 x 152.4 mm) - same as WRAP.1E • Firmware: tinyBIOS
Customer options	I2C bus, buzzer, RTC battery
Changes from ALIX.2C	• Increase USB current limit. • USB headers as build option. • USB ports 3 and 4 on header (not tested). • Change optional serial header J12 to COM2. • Add LED and switch pins to I2C header. • Populate buzzer driver circuit, add pins for use as GPIO. • Add option for power in header J18. • Some enhancements to reduce EMI. • Add second POSCAP to ruggedize 3.3V rail for high power radio cards.
Manufacturer	PC Engines
Origin	Taiwan

4:09 PM





Firewall Bypassing Methods and Techniques

BYPASSING PARAMETER VERIFICATION

- PHP removeswhitespacesfromparameternamesortransformsthemintounderscores

  http://www.website.com/products.php?%20productid=select 1,2,3

- ASP removes % character that is not followed by two hexadecimal digits

  http://www.website.com/products.aspx?%productid=select 1,2,3

- A WAF which does not reject unknown parameters may be bypassed with this technique.

PRE-PROCESSOR EXPLOITATION

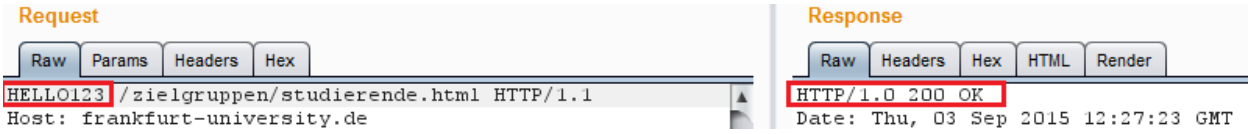
X-* Headers

- WAF maybeconfiguredtotrustcertaininternal IP Addresses
- Input validationisnot appliedon requestsoriginatingfromtheseIPs
- IfWAF retrievestheseIPs fromheaderswhichcanbechangedbya usera bypassmayoccur
- A user is in control of the following HTTP Headers:

1. X-Originating-IP
2. X-Forwarded-For
3. X-Remote-IP
4. X-Remote-Addr

MALFORMED HTTP METHOD

- Misconfiguredweb serversmayacceptmalformedHTTP methods



- A WAF thatonlyinspectsGET andPOST requestsmaybebypassed

OVERLOADING THE WAF

- A WAF maybeconfiguredtoskipinputvalidationifperformanceloadisheavy
- OftenappliestoembeddedWAFs
- Great deal ofmaliciousrequestscanbesentwiththechancethattheWAF will overloadandskipsomerequests

HTTP PARAMETER POLLUTION

- Sending a number of parameters with the same name
- Technologies interpret this request

http://www.website.com/products/?productid=1&productid=2

Back end	Behavior	Processed
ASP.NET	Concatenate with comma	productid=1,2
JSP	First Occurrence	productid=1
PHP	Last Occurrence	productid=2

IMPEDANCE MISMATCH

The following payload

?productid=select 1,2,3from table

Can be divided:

?productid=select1&productid=2,3 from table

- WAF sees two individual parameters and may not detect the payload
- ASP.NET back end concatenates both values

HTTP PARAMETER FRAGMENTATION

- Splitting subsequent code between different parameters
- Example query:

sql= "SELECT * FROM table WHERE uid= "+$_GET['uid']+" and pid= +$_GET[‘pid']“

- The following request:

http://www.website.com/index.php?uid=1+union/*&pid=*/select 1,2,3

would result in this SQL Query:

sql= "SELECT * FROM table WHERE uid= 1union/* and pid= */select 1,2,3"

DOUBLE URL ENCODING

- WAF normalizes URL encoded characters into ASCII text
- The WAF may be configured to decode characters only once
- Double URL Encoding a payload may result in a bypass

  ’s’ -> %73 -> %25%37%33

- The following payload contains a double URL encoded character

  1 union%25%37%33elect 1,2,3

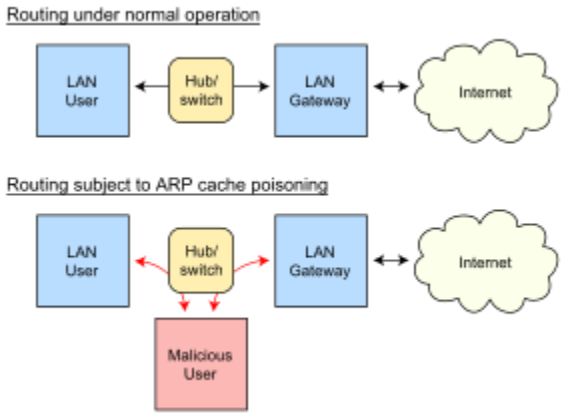
Network Attacks

ARP spoofing

In computer networking, ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks.

The attack can only be used on networks that use the Address Resolution Protocol, and is limited to local network segments.



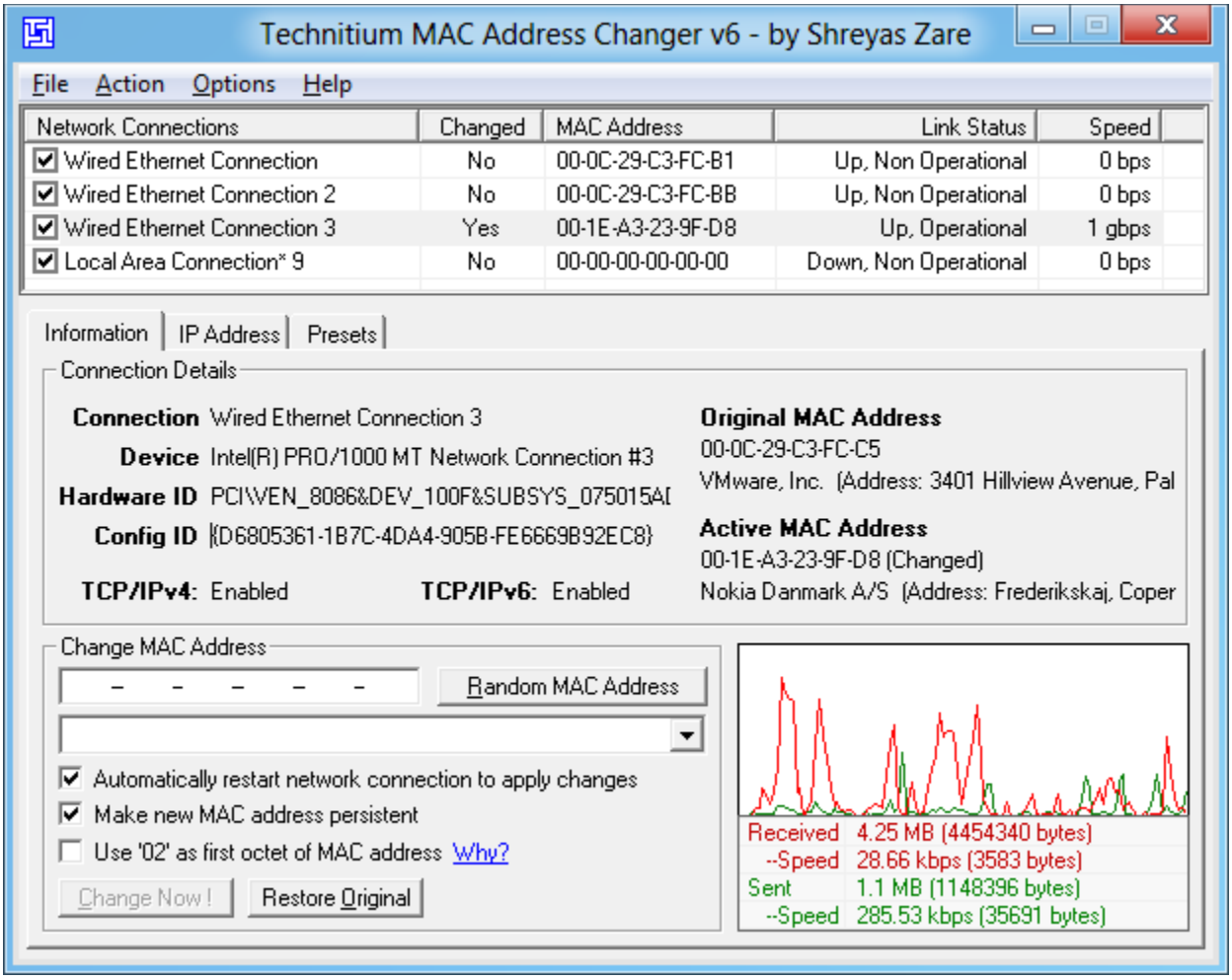
Anatomy of an ARP spoofing attack

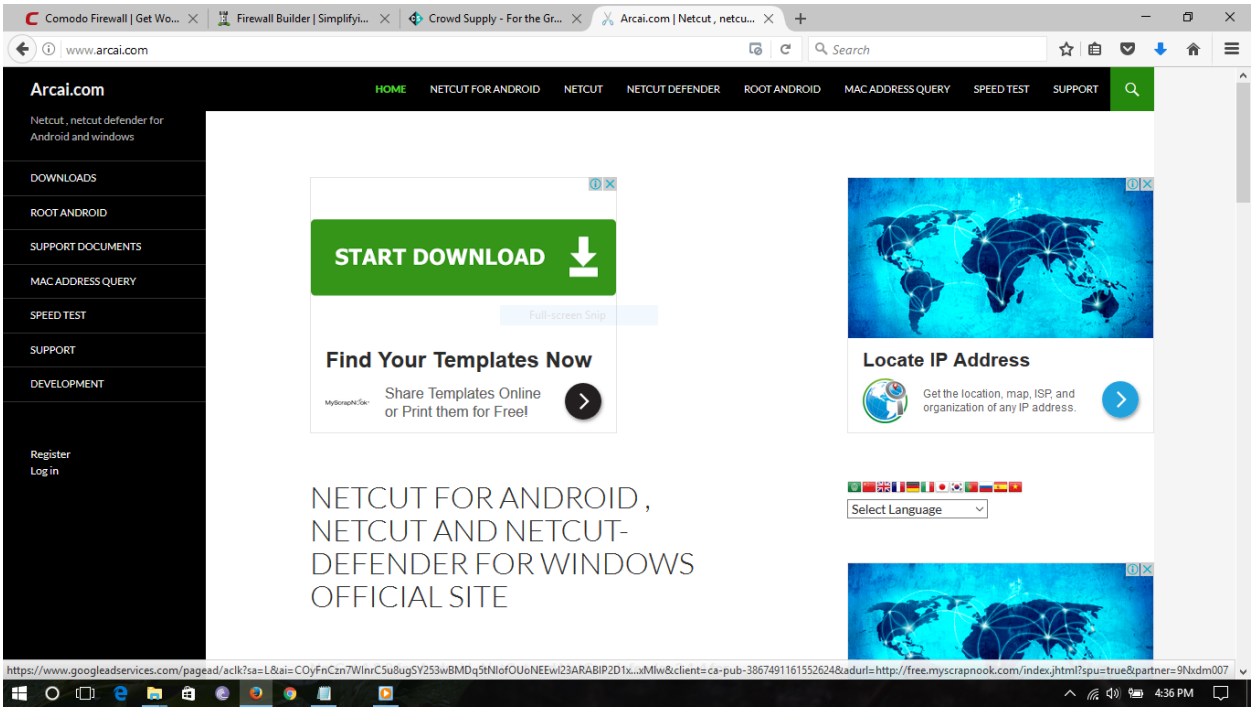
The basic principle behind ARP spoofing is to exploit the lack of authentication in the ARP protocol by sending spoofed ARP messages onto the LAN. ARP spoofing attacks can be run from a compromised host on the LAN, or from an attacker's machine that is connected directly to the target LAN.

Generally, the goal of the attack is to associate the attacker's host MAC address with the IP address of a target host, so that any traffic meant for the target host will be sent to the attacker's host. The attacker may choose to inspect the packets (spying), while forwarding the traffic to the actual default destination to avoid discovery, modify the data before forwarding it (man-in-the-middle attack), or launch a denial-of-service attack by causing some or all of the packets on the network to be dropped.

ARP spoofing tools Eg:

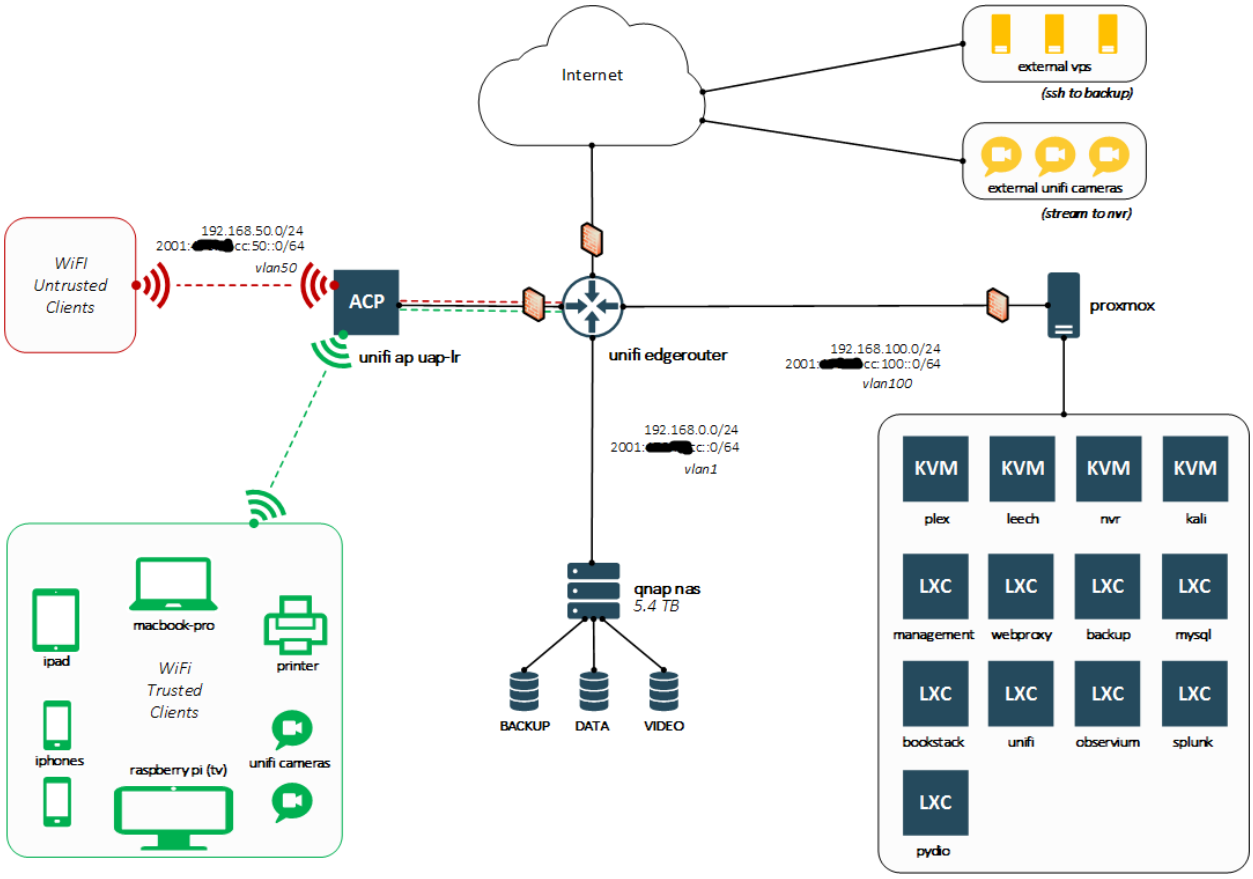
T MAC




Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
Crowd Supply - For the Gr...
Arcai.com | Netcut , netcu...
www.arcai.com
Search
Arcai.com
Netcut , netcut defender for Android and windows
HOME
NETCUT FOR ANDROID
NETCUT
NETCUT DEFENDER
ROOT ANDROID
MAC ADDRESS QUERY
SPEED TEST
SUPPORT
DOWNLOADS
ROOT ANDROID
SUPPORT DOCUMENTS
MAC ADDRESS QUERY
SPEED TEST
SUPPORT
DEVELOPMENT
Register
Log in
START DOWNLOAD
Find Your Templates Now
Share Templates Online or Print them for Free!
Locate IP Address
Get the location, map, ISP, and organization of any IP address.
Select Language
NETCUT FOR ANDROID , NETCUT AND NETCUT-DEFENDER FOR WINDOWS OFFICIAL SITE
https://www.googleadservices.com/pagead/aclk?sa=L&ai=COyFnCzn7WInrC5u8ugSY253wBMDq5tNIofOUoNEEwl23ARABIP2D1x...xMlw&client=ca-pub-3867491161552624&adurl=http://free.myscrapnook.com/index.jhtml?spu=true&partner=9Nxdm007
4:36 PM

Netcut

Effective Network Isolation



Enabling DHCP Snooping Globally

To enable DHCP snooping globally, perform this task:

	Command	Purpose
Step 1	Router(config)# ip dhcp snooping	Enables DHCP snooping globally.
Step 2	Router(config)# do show ip dhcp snooping | include Switch	Verifies the configuration.

This example shows how to enable DHCP snooping globally:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping
Router(config)# do show ip dhcp snooping | include Switch
Switch DHCP snooping is enabled
Router(config)#
```

Enabling DHCP Option-82 Data Insertion

To enable DHCP option-82 data insertion, perform this task:

	Command	**Purpose**
Step 1	Router(config)# **ip dhcp snooping information option**	Enables DHCP option-82 data insertion.
Step 2	Router(config)# **ip dhcp snooping information option replace** Or: Router(config-if)# **ip dhcp snooping information option replace**	(Optional) Replaces the DHCP relay information option received in snooped packets with the switch's option-82 data. Available in releases where CSCto29645 is resolved and when DHCP option-82 data insertion is enabled.
Step 3	Router(config)# **do show ip dhcp snooping | include 82**	Verifies the configuration.

This example shows how to disable DHCP option-82 data insertion:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no ip dhcp snooping information option
Router(config)# do show ip dhcp snooping | include 82
Insertion of option 82 is disabled
Router(config)#
```

This example shows how to enable DHCP option-82 data insertion:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping information option
Router(config)# do show ip dhcp snooping | include 82
Insertion of option 82 is enabled
Router(config)#
```

Enabling DHCP Snooping Host Tracking

To configure the DHCP snooping host tracking feature, perform one or more of the following tasks:

Command	**Purpose**
Router(config)# **ip dhcp snooping track host**	Enables the DHCP snooping host tracking feature.
Router# **show ip dhcp snooping track host**	Displays the contents of the DHCP snooping host tracking cache.
Router# **show ip dhcp snooping track host statistics**	Displays the DHCP snooping host track statistics.
Router# **clear ip dhcp snooping track host**	Clears the DHCP snooping host track cache.
Router# **clear ip dhcp snooping track hosts statistics**	Clears the DHCP snooping host track statistics.

This example shows how to enable the DHCP snooping host tracking feature:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no ip dhcp snooping information option
Router(config)# ip dhcp snooping track host
Router(config)# exit
```

This example shows how to display the contents of the DHCP snooping host tracking cache:

```
Router# show ip dhcp snooping track host
VLAN   interface     mac           time left
 ------------------------------------------
 203     Gi3/47      000a.cb00.126d     expired
 204     Gi11/47     000a.cc00.1262     expired
 202     Gi2/47      000a.ca00.125d     expired
 204     Gi11/47     000a.cc00.1263     expired
 203     Gi3/47      000a.cb00.1276     expired
```

```
 201      Gi1/47      000a.c900.1273     expired
```

This example shows how to display the statistics associated with DHCP snooping host tracking feature:

```
Router# show ip dhcp snooping track host statistics
DHCP host track entries            = 168
DHCP host track hits               = 34028
DHCP host track misses             = 0
DHCP host track limit exceeded     = 0
```

Enabling DHCP Snooping MAC Address Verification

With DHCP snooping MAC address verification enabled, DHCP snooping verifies that the source MAC address and the client hardware address match in DHCP packets that are received on untrusted ports. The source MAC address is a Layer 2 field associated with the packet, and the client hardware address is a Layer 3 field in the DHCP packet.

To enable DHCP snooping MAC address verification, perform this task:

	Command	Purpose
Step 1	Router(config)# ip dhcp snooping verify mac-address	Enables DHCP snooping MAC address verification.
Step 2	Router(config)# do show ip dhcp snooping | include hwaddr	Verifies the configuration.

This example shows how to disable DHCP snooping MAC address verification:

```
Router(config)# no ip dhcp snooping verify mac-address
Router(config)# do show ip dhcp snooping | include hwaddr
Verification of hwaddr field is disabled
Router(config)#
```

This example shows how to enable DHCP snooping MAC address verification:

```
Router(config)# ip dhcp snooping verify mac-address
Router(config)# do show ip dhcp snooping | include hwaddr
Verification of hwaddr field is enabled
Router(config)#
```

Enabling DHCP Snooping on VLANs

By default, the DHCP snooping feature is inactive on all VLANs. You may enable the feature on a single VLAN or a range of VLANs.

When enabled on a VLAN, the DHCP snooping feature creates four entries in the VACL table in the MFC3. These entries cause the PFC3 to intercept all DHCP messages on this VLAN and send them to the RP. The DHCP snooping feature is implemented in software on the RP.

To enable DHCP snooping on VLANs, perform this task:

	Command	Purpose
Step 1	Router(config)# ip dhcp snooping vlan {{*vlan_ID* [*vlan_ID*]} | {*vlan_range*}	Enables DHCP snooping on a VLAN or VLAN range.
Step 2	Router(config)# do show ip dhcp snooping	Verifies the configuration.

You can configure DHCP snooping for a single VLAN or a range of VLANs:

- To configure a single VLAN, enter a single VLAN number.
- To configure a range of VLANs, enter a beginning and an ending VLAN number or a dash-separated pair of VLAN numbers.
- You can enter a comma-separated list of VLAN numbers and dash-separated pairs of VLAN numbers.

This example shows how to enable DHCP snooping on VLANs 10 through 12:

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10 12
Router(config)#
```

This example shows another way to enable DHCP snooping on VLANs 10 through 12:

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10-12
```

This example shows another way to enable DHCP snooping on VLANs 10 through 12:

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10,11,12
```

This example shows how to enable DHCP snooping on VLANs 10 through 12 and VLAN 15:

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10-12,15
```

This example shows how to verify the configuration:

```
Router(config)# do show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10-12,15
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following Interfaces:
Insertion of option 82 is enabled
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
Router#
```

Configuring Spurious DHCP Server Detection

To detect and locate spurious DHCP servers, perform this task:

	Command	Purpose
Step 1	Router(config)# ip dhcp snooping detect spurious vlan *range*	Enables detection of spurious DHCP servers on a specified VLAN range.
Step 2	Router(config)# ip dhcp snooping detect spurious interval *time*	Sets the interval time, the default is 30 minutes.
Step 3	Router# show ip dhcp snooping detect spurious	Verifies spurious DHCP server detection.

This example shows how to configure DHCP spurious server detection on VLANs 20 to 25 and set the interval to 50 minutes:

```
Router# configure terminal
Router(config)# ip dhcp snooping detect spurious vlan 20-25
Router(config)# ip dhcp snooping detect spurious interval 50
Router# do show ip dhcp snooping detect spurious
Spurious DHCP server detection is enabled.
Detection VLAN list : 20-25
Detection interval : 50 minutes
Router#
```

Configuring the DHCP Snooping Database Agent

To configure the DHCP snooping database agent, perform one or more of the following tasks:

Command	Purpose
`Router(config)# ip dhcp snooping database { _url | write-delay seconds | timeout seconds }`	Configures a URL for the database agent (or file) and the related timeout values.
`Router# show ip dhcp snooping database [detail]`	Displays the current operating state of the database agent and statistics associated with the transfers.
`Router# clear ip dhcp snooping database statistics`	Clears the statistics associated with the database agent.
`Router# renew ip dhcp snooping database [validation none] [url]`	Requests the read entries from a file at the given URL.
`Router# ip dhcp snooping binding mac_address vlan vlan_ID ip_address interface ifname expiry lease_in_seconds`	Adds bindings to the snooping database.

Reading Binding Entries from a TFTP File

To manually read the entries from a TFTP file, perform this task:

	Command	Purpose
Step 1	`Router# show ip dhcp snooping database`	Displays the DHCP snooping database agent statistics.
Step 2	`Router# renew ip dhcp snoop data` *`url`*	Directs the switch to read the file from the URL.
Step 3	`Router# show ip dhcp snoop data`	Displays the read status.
Step 4	`Router# show ip dhcp snoop bind`	Verifies whether the bindings were read successfully.

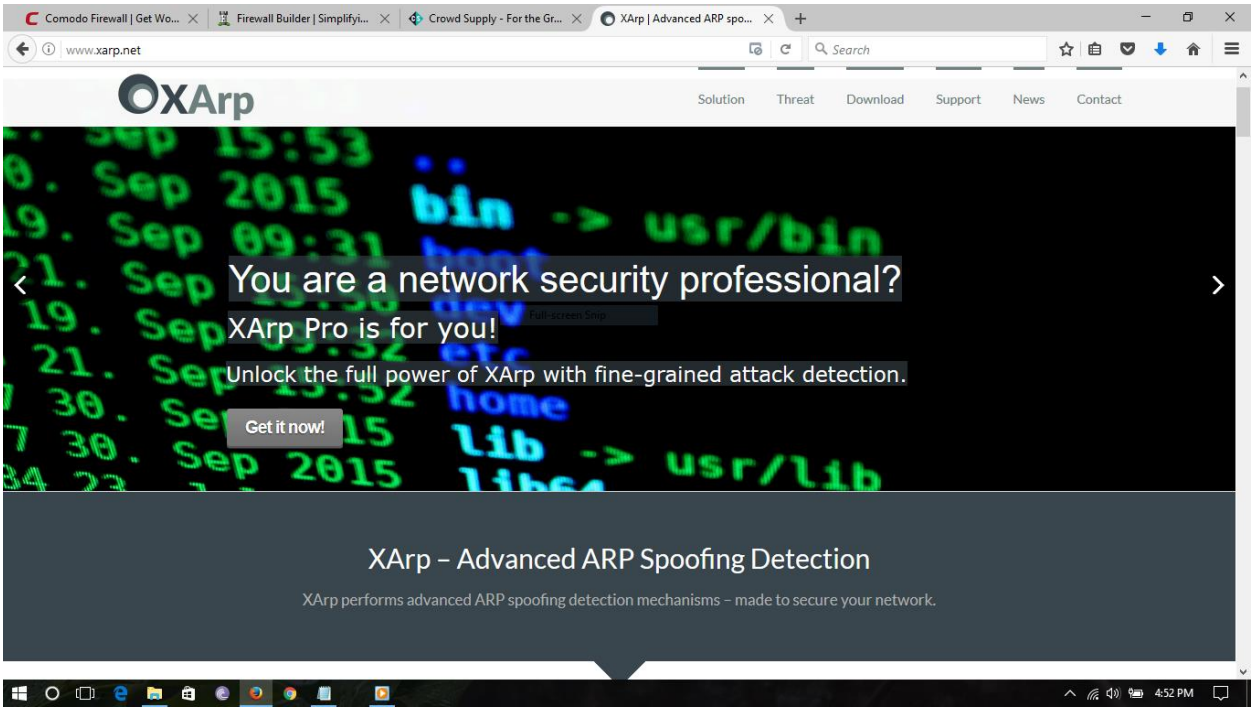
This is an example of how to manually read entries from the tftp://10.1.1.1/directory/file:

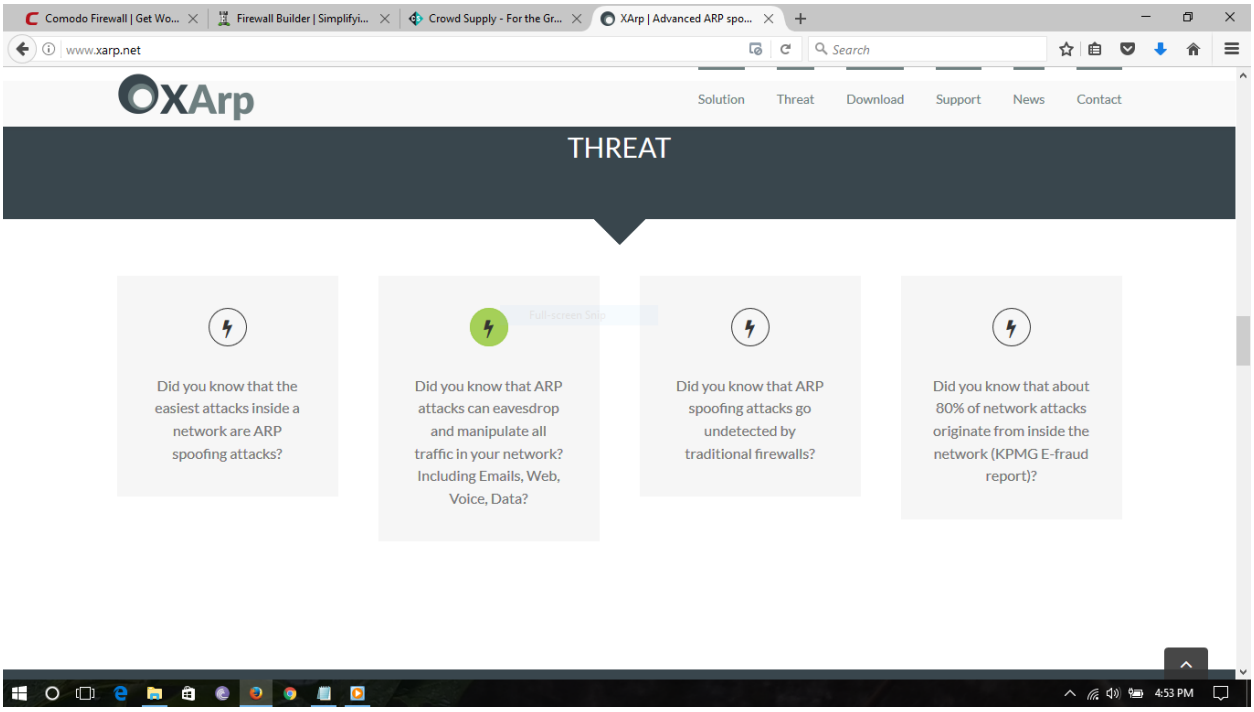
```
Router# show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running
Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Router# renew ip dhcp snoop data tftp://10.1.1.1/directory/file
Loading directory/file from 10.1.1.1 (via GigabitEthernet1/1): !
[OK - 457 bytes]
Database downloaded successfully.
Router#
00:01:29: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database
Read
```

```
succeeded.
Router# show ip dhcp snoop data
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running
Last Succeeded Time : 15:24:34 UTC Sun Jul 8 2001
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts       :        1   Startup Failures :        0
Successful Transfers :        1   Failed Transfers :        0
Successful Reads     :        1   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Router#
Router# show ip dhcp snoop bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN
Interface
------------------  ---------------  ----------  -------------  ----  -------
-------------
00:01:00:01:00:05   1.1.1.1          49810       dhcp-snooping  512
GigabitEthernet1/1
00:01:00:01:00:02   1.1.1.1          49810       dhcp-snooping  512
GigabitEthernet1/1
00:01:00:01:00:04   1.1.1.1          49810       dhcp-snooping  1536
GigabitEthernet1/1
00:01:00:01:00:03   1.1.1.1          49810       dhcp-snooping  1024
GigabitEthernet1/1
00:01:00:01:00:01   1.1.1.1          49810       dhcp-snooping  1
GigabitEthernet1/1
Router# clear ip dhcp snoop bind
Router# show ip dhcp snoop bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN
Interface
------------------  ---------------  ----------  -------------  ----  -------
-------------
Router#
```

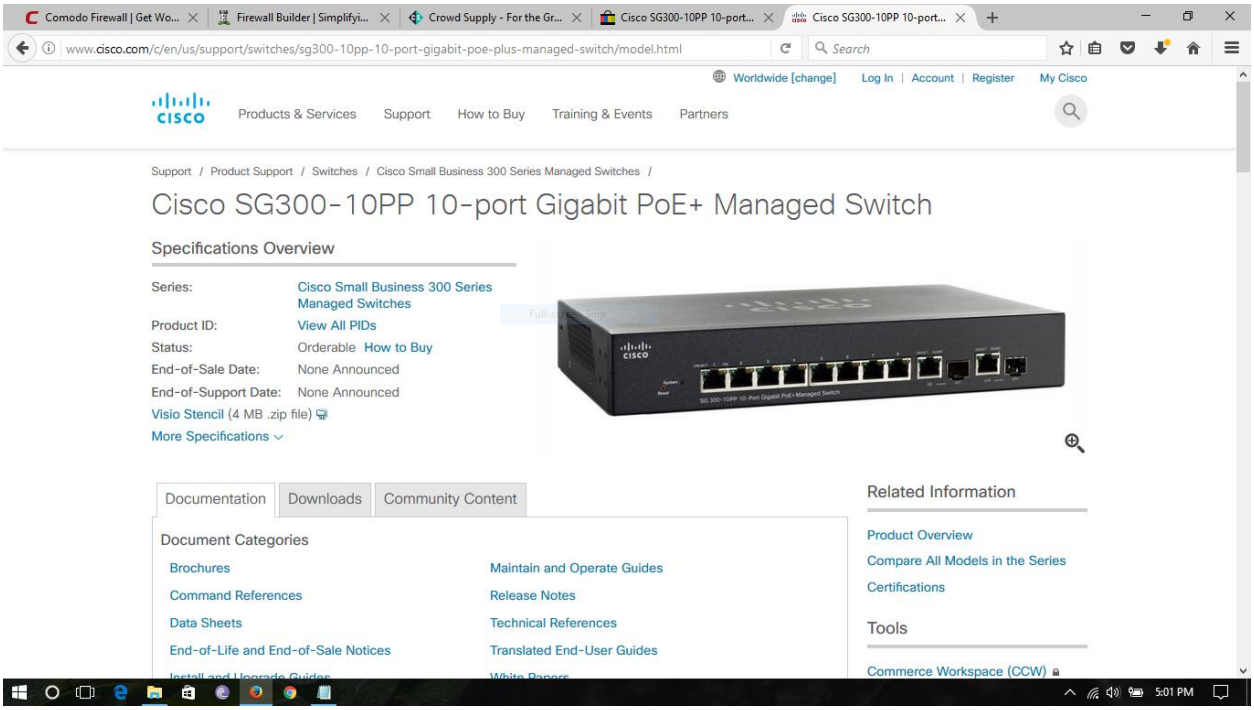
ARP spoofing detection:

XArp





CISCO


Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
Crowd Supply - For the Gr...
Cisco SG300-10PP 10-port...
Cisco SG300-10PP 10-port...
www.cisco.com/c/en/us/support/switches/sg300-10pp-10-port-gigabit-poe-plus-managed-switch/model.html
Search
Worldwide [change]
Log In | Account | Register
My Cisco
Products & Services
Support
How to Buy
Training & Events
Partners
Support / Product Support / Switches / Cisco Small Business 300 Series Managed Switches /
Cisco SG300-10PP 10-port Gigabit PoE+ Managed Switch
Specifications Overview
Series: Cisco Small Business 300 Series Managed Switches
Product ID: View All PIDs
Status: Orderable How to Buy
End-of-Sale Date: None Announced
End-of-Support Date: None Announced
Visio Stencil (4 MB .zip file)
More Specifications
Documentation
Downloads
Community Content
Document Categories
Brochures
Command References
Data Sheets
End-of-Life and End-of-Sale Notices
Maintain and Operate Guides
Release Notes
Technical References
Translated End-User Guides
Related Information
Product Overview
Compare All Models in the Series
Certifications
Tools
Commerce Workspace (CCW)
5:01 PM

Network Monitoring for Threats

Syslog

In computing, syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.

Computer system designers may use syslog for system management and security auditing as well as general informational, analysis, and debugging messages. A wide variety of devices, such as printers, routers, and message receivers across many platforms use the syslog standard. This permits the consolidation of logging data from different types of systems in a central repository. Implementations of syslog exist for many operating systems.

A facility code is used to specify the type of program that is logging the message. Messages with different facilities may be handled differently. The list of facilities available is defined by RFC 3164.

Facility code	Keyword	Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9		clock daemon
10	authpriv	security/authorization messages

11	ftp	FTP daemon
12	-	NTP subsystem
13	-	log audit
14	-	log alert
15	cron	scheduling daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

The list of severities is also defined by RFC 5424.

Value	Severity	Keyword	Deprecated keywords	Description
0	Emergency	`emerg`	`panic`	System is unusable. A panic condition.
1	Alert	`alert`		Action must be taken immediately. A condition that should be corrected immediately, such as a corrupted system database.
2	Critical	`crit`		Critical conditions, such as hard device errors.
3	Error	`err`	`error`	Error conditions.

4	Warning	`warning`	`warn`	Warning conditions.
5	Notice	`notice`		Normal but significant conditions. Conditions that are not error conditions, but that may require special handling.
6	Informational	`info`		Informational messages.
7	Debug	`debug`		Debug-level messages. Messages that contain information normally of use only when debugging a program.

RSYSLOG

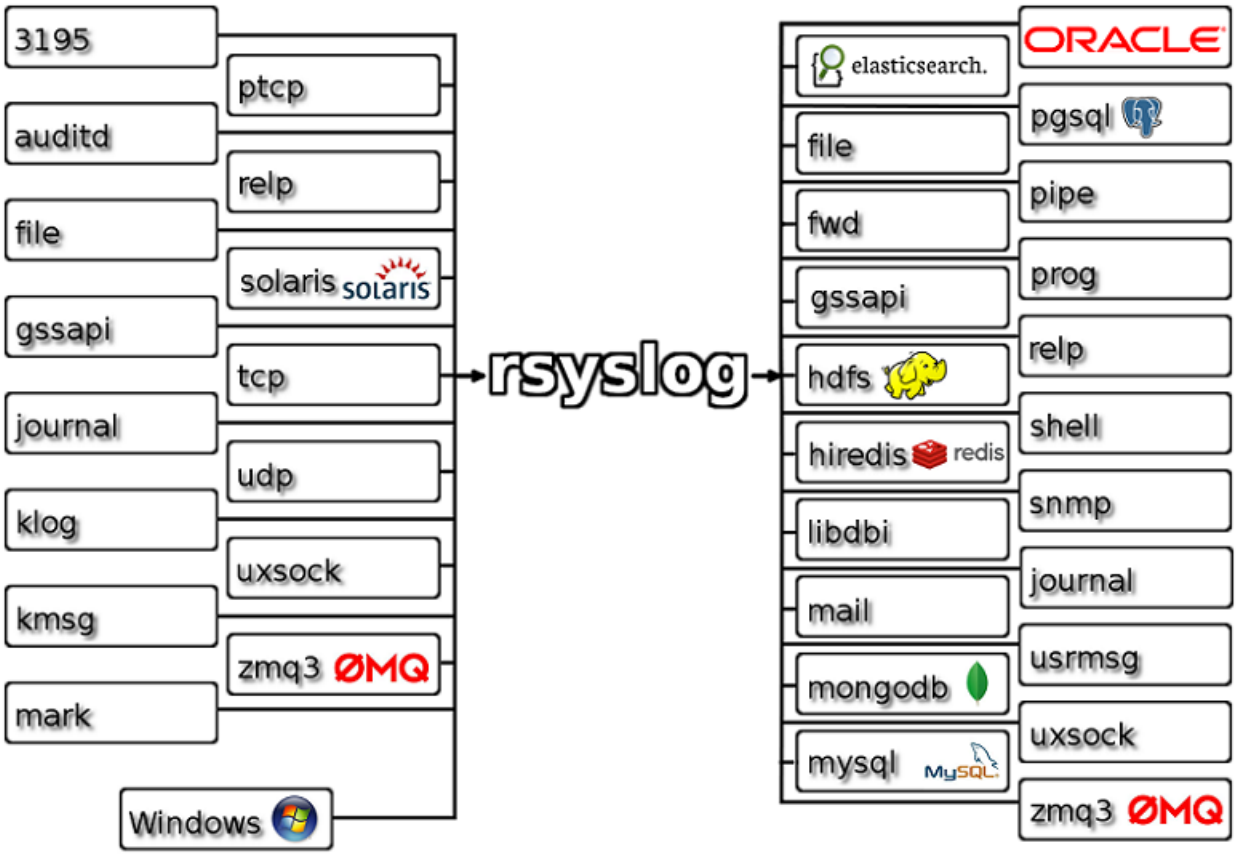
RSYSLOG is the rocket-fast system for log processing.

It offers high-performance, great security features and a modular design. While it started as a regular syslogd, rsyslog has evolved into a kind of swiss army knife of logging, being able to accept inputs from a wide variety of sources, transform them, and output to the results to diverse destinations.

RSYSLOG can deliver over one million messages per second to local destinations when limited processing is applied (based on v7, December 2013). Even with remote destinations and more elaborate processing the performance is usually considered "stunning".

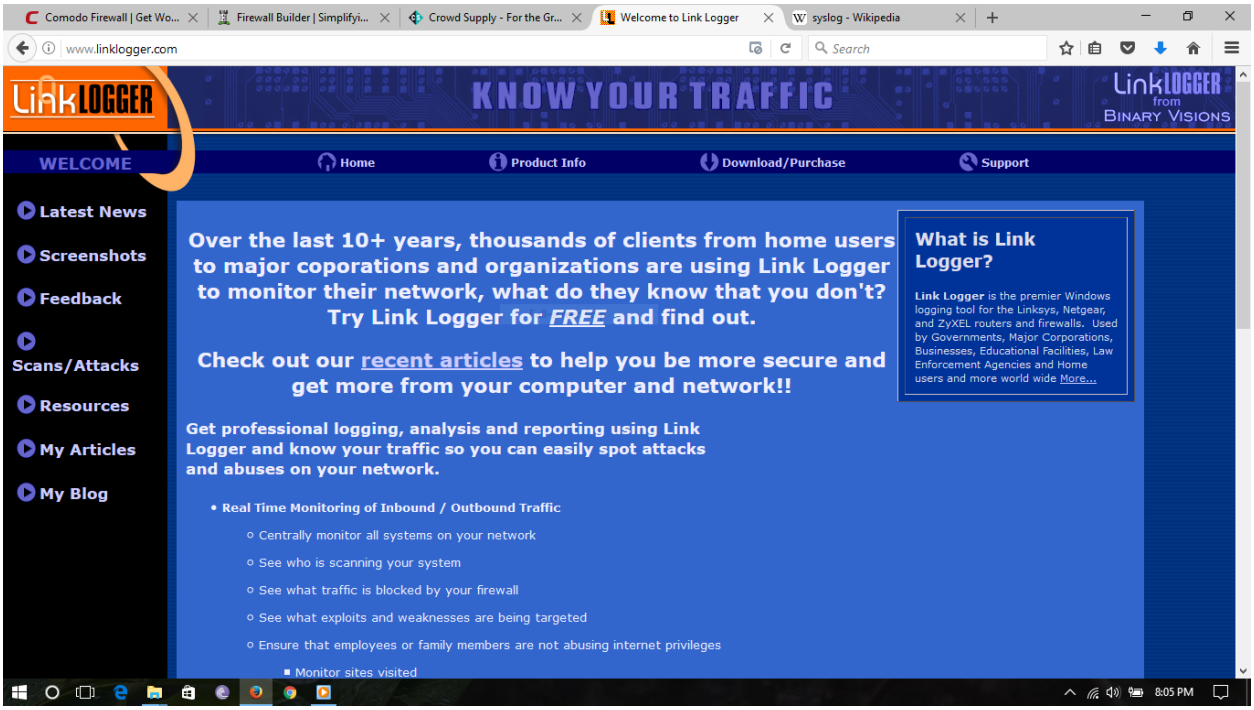
RSYSLOG:

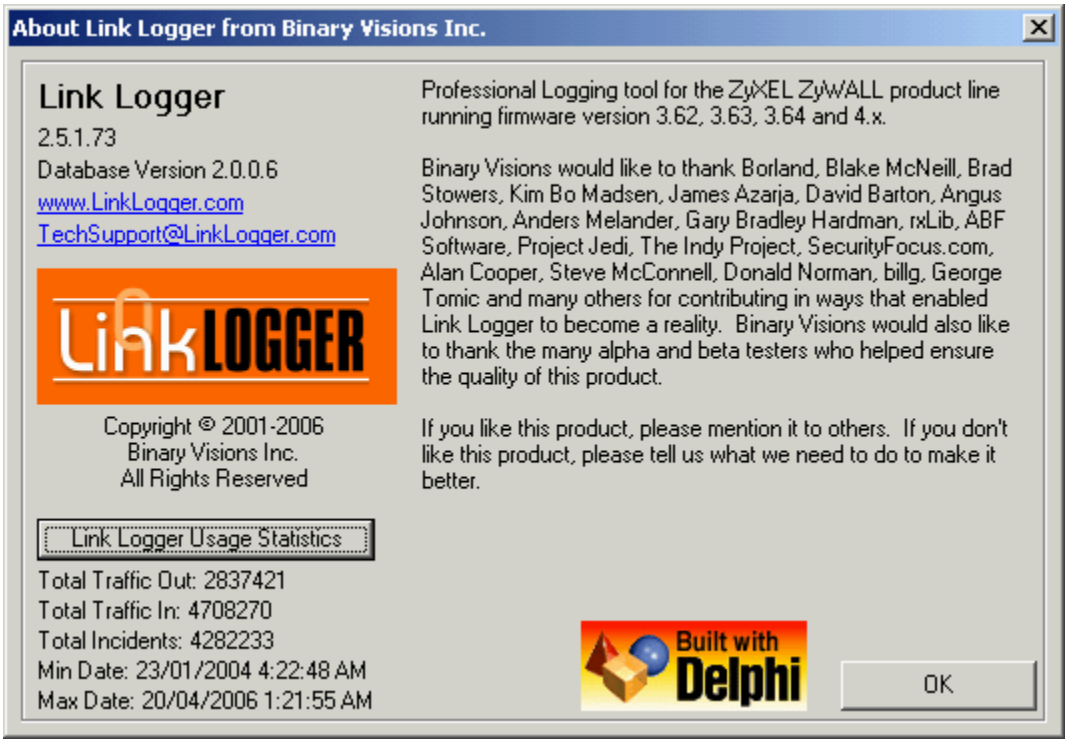
- Multi-threading
- TCP, SSL, TLS, RELP
- MySQL, PostgreSQL, Oracle and more
- Filter any part of syslog message
- Fully configurable output format
- Suitable for enterprise-class relay chains


3195
auditd
file
gssapi
journal
klog
kmsg
mark
ptcp
relp
solaris
tcp
udp
uxsock
zmq3
Windows
rsyslog
elasticsearch.
file
fwd
gssapi
hdfs
hiredis
redis
libdbi
mail
mongodb
mysql
ORACLE
pgsql
pipe
prog
relp
shell
snmp
journal
usrmsg
uxsock
zmq3

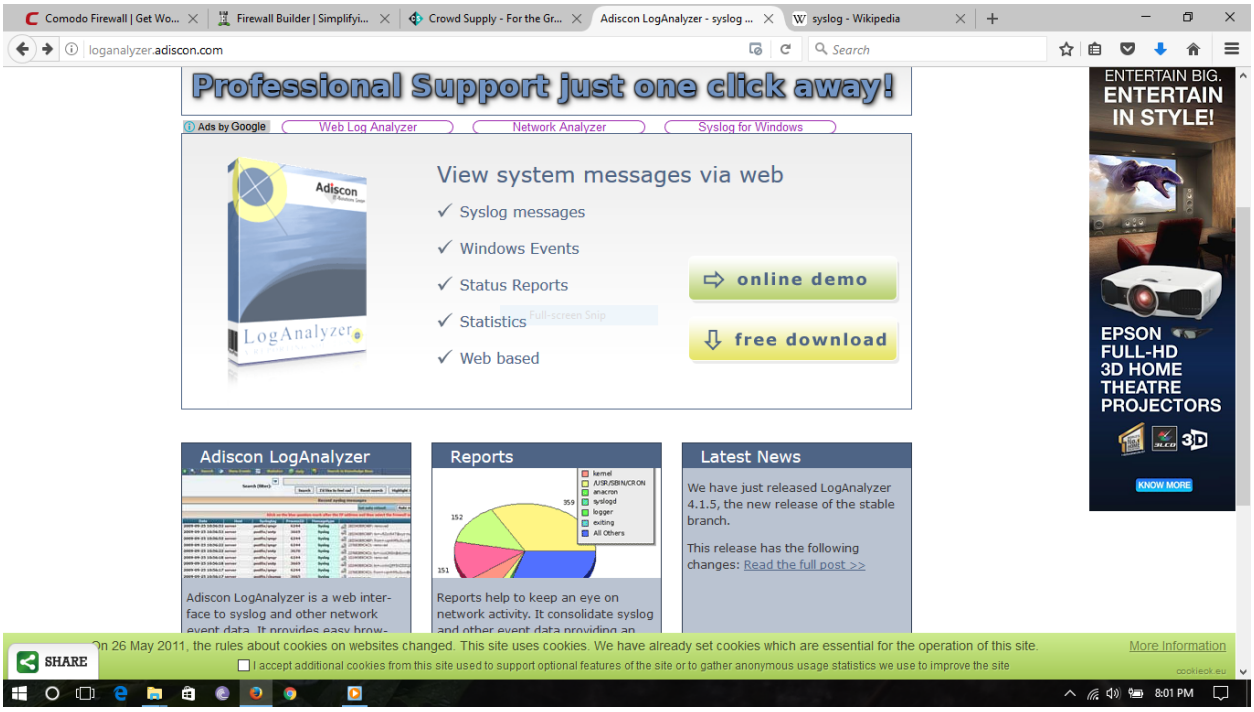
Tools:

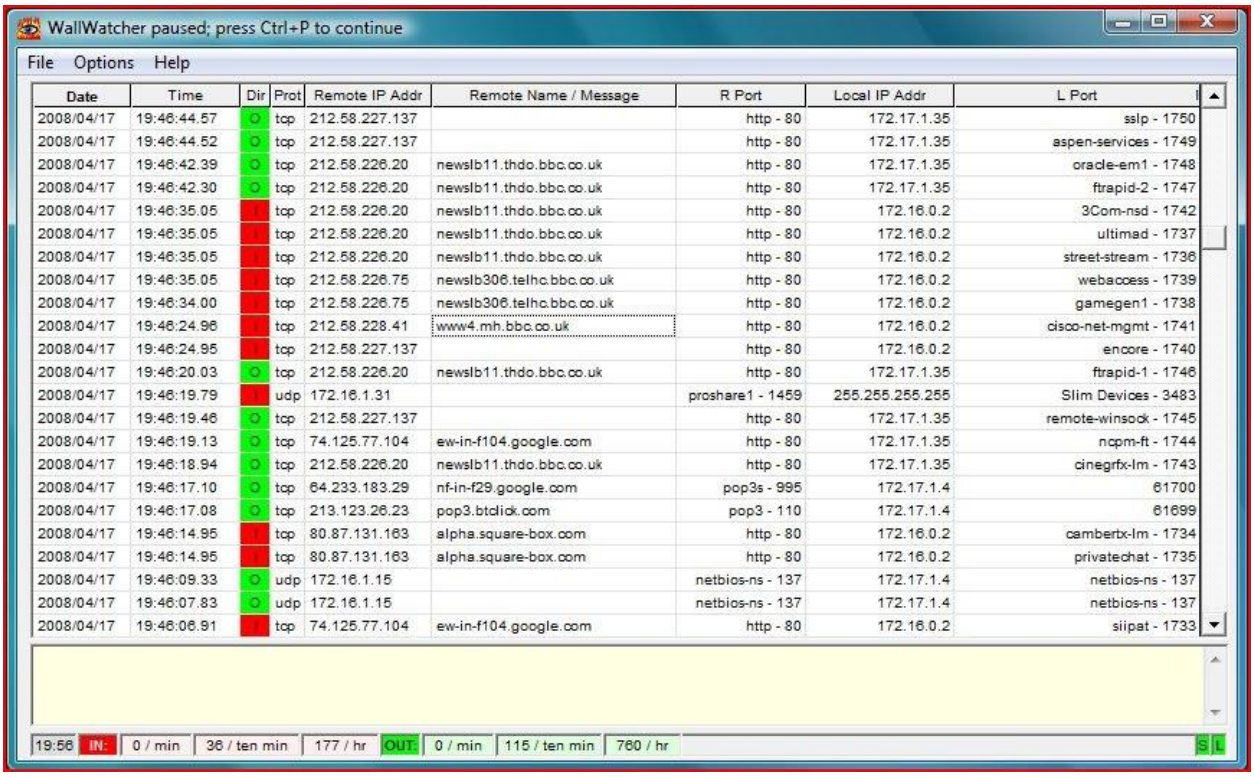
Linklogger





Loganalyzer





Wallwatcher

Malware and Hackers

Wireshark

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named **Ethereal**, the project was renamed Wireshark in May 2006 due to trademark issues.

Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

Wireshark is a data capturing program that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.

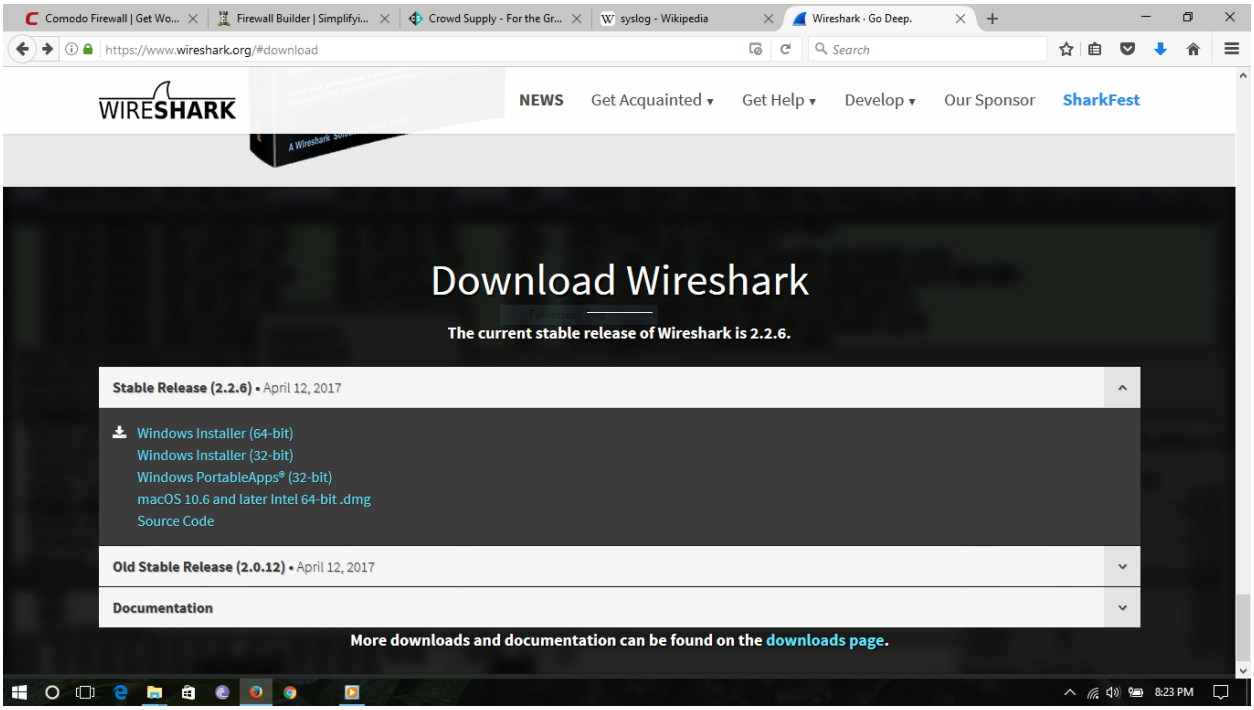
- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- Data display can be refined using a display filter.
- Plug-ins can be created for dissecting new protocols.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured.
- Wireless connections can also be filtered as long as they traverse the monitored Ethernet.
- Various settings, timers, and filters can be set that ensure only triggered traffic appear.

Wireshark's native network trace file format is the libpcap format supported by libpcap and WinPcap, so it can exchange captured network traces with other applications that use the same format, including tcpdump and CA NetMaster. It can also read captures from other network analyzers, such as snoop, Network General's Sniffer, and Microsoft Network Monitor.

Capturing raw network traffic from an interface requires elevated privileges on some platforms. For this reason, older versions of Ethereal/Wireshark and tethereal/TShark often ran with superuser privileges. Taking into account the huge number of protocol dissectors that are called when traffic is captured, this can pose a serious security risk given the possibility of a bug in a dissector. Due to the rather large number of vulnerabilities in the past (of which many have allowed remote code execution) and developers' doubts for better future development, OpenBSD removed Ethereal from its ports tree prior to OpenBSD 3.6.

Elevated privileges are not needed for all operations. For example, an alternative is to run tcpdump or the dumpcap utility that comes with Wireshark with superuser privileges to capture packets into a file, and later analyze the packets by running Wireshark with restricted privileges. To emulate near realtime analysis, each captured file may be merged by mergecap into growing file processed by Wireshark. On wireless networks, it is possible to use the Aircrack wireless security tools to capture IEEE 802.11 frames and read the resulting dump files with Wireshark.

As of Wireshark 0.99.7, Wireshark and TShark run dumpcap to perform traffic capture. Platforms that require special privileges to capture traffic need only dumpcap run with those privileges. Neither Wireshark nor TShark need to or should be run with special privileges.



Wireshark Display Filters · Part 1

packetlife.net

Ethernet

eth.addr	eth.len	eth.src
eth.dst	eth.lg	eth.trailer
eth.ig	eth.multicast	eth.type

IEEE 802.1Q

vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer

IPv4

ip.addr	ip.fragment.overlap.conflict
ip.checksum	ip.fragment.toolongfragment
ip.checksum_bad	ip.fragments
ip.checksum_good	ip.hdr_len
ip.dsfield	ip.host
ip.dsfield.ce	ip.id
ip.dsfield.dscp	ip.len
ip.dsfield.ect	ip.proto
ip.dst	ip.reassembled_in
ip.dst_host	ip.src
ip.flags	ip.src_host
ip.flags.df	ip.tos
ip.flags.mf	ip.tos.cost
ip.flags.rb	ip.tos.delay
ip.frag_offset	ip.tos.precedence
ip.fragment	ip.tos.reliability
ip.fragment.error	ip.tos.throughput
ip.fragment.multipletails	ip.ttl
ip.fragment.overlap	ip.version

IPv6

ipv6.addr	ipv6.hop_opt
ipv6.class	ipv6.host
ipv6.dst	ipv6.mipv6_home_address
ipv6.dst_host	ipv6.mipv6_length
ipv6.dst_opt	ipv6.mipv6_type
ipv6.flow	ipv6.nxt
ipv6.fragment	ipv6.opt.pad1
ipv6.fragment.error	ipv6.opt.padn
ipv6.fragment.more	ipv6.plen
ipv6.fragment.multipletails	ipv6.reassembled_in
ipv6.fragment.offset	ipv6.routing_hdr
ipv6.fragment.overlap	ipv6.routing_hdr.addr
ipv6.fragment.overlap.conflict	ipv6.routing_hdr.left
ipv6.fragment.toolongfragment	ipv6.routing_hdr.type
ipv6.fragments	ipv6.src
ipv6.fragment.id	ipv6.src_host
ipv6.hlim	ipv6.version

ARP

arp.dst.hw_mac	arp.proto.size
arp.dst.proto_ipv4	arp.proto.type
arp.hw.size	arp.src.hw_mac
arp.hw.type	arp.src.proto_ipv4
arp.opcode	

TCP

tcp.ack	tcp.options.qs
tcp.checksum	tcp.options.sack
tcp.checksum_bad	tcp.options.sack_le
tcp.checksum_good	tcp.options.sack_perm
tcp.continuation_to	tcp.options.sack_re
tcp.dstport	tcp.options.time_stamp
tcp.flags	tcp.options.wscale
tcp.flags.ack	tcp.options.wscale_val
tcp.flags.cwr	tcp.pdu.last_frame
tcp.flags.ecn	tcp.pdu.size
tcp.flags.fin	tcp.pdu.time
tcp.flags.push	tcp.port
tcp.flags.reset	tcp.reassembled_in
tcp.flags.syn	tcp.segment
tcp.flags.urg	tcp.segment.error
tcp.hdr_len	tcp.segment.multipletails
tcp.len	tcp.segment.overlap
tcp.nxtseq	tcp.segment.overlap.conflict
tcp.options	tcp.segment.toolongfragment
tcp.options.cc	tcp.segments
tcp.options.ccecho	tcp.seq
tcp.options.ccnew	tcp.srcport
tcp.options.echo	tcp.time_delta
tcp.options.echo_reply	tcp.time_relative
tcp.options.md5	tcp.urgent_pointer
tcp.options.mss	tcp.window_size
tcp.options.mss_val	

UDP

udp.checksum	udp.dstport	udp.srcport
udp.checksum_bad	udp.length	
udp.checksum_good	udp.port	

Operators

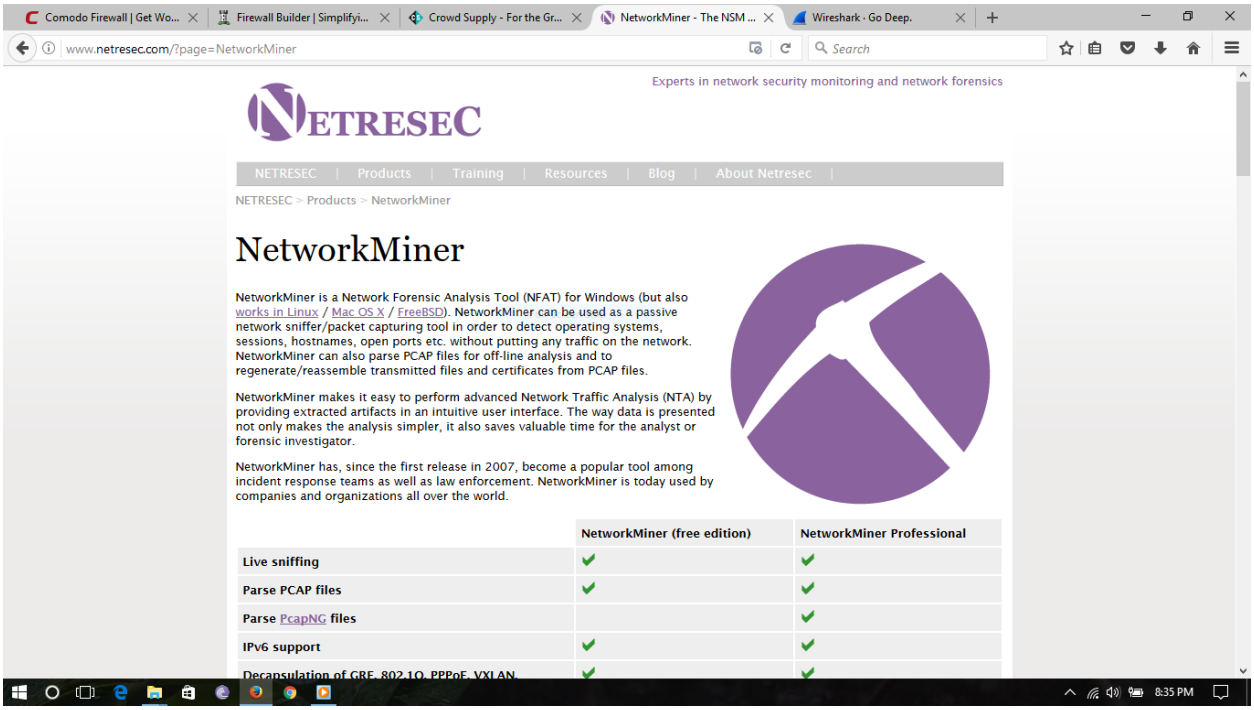
eq or ==	
ne or !=	
gt or >	
lt or <	
ge or >=	
le or <=	

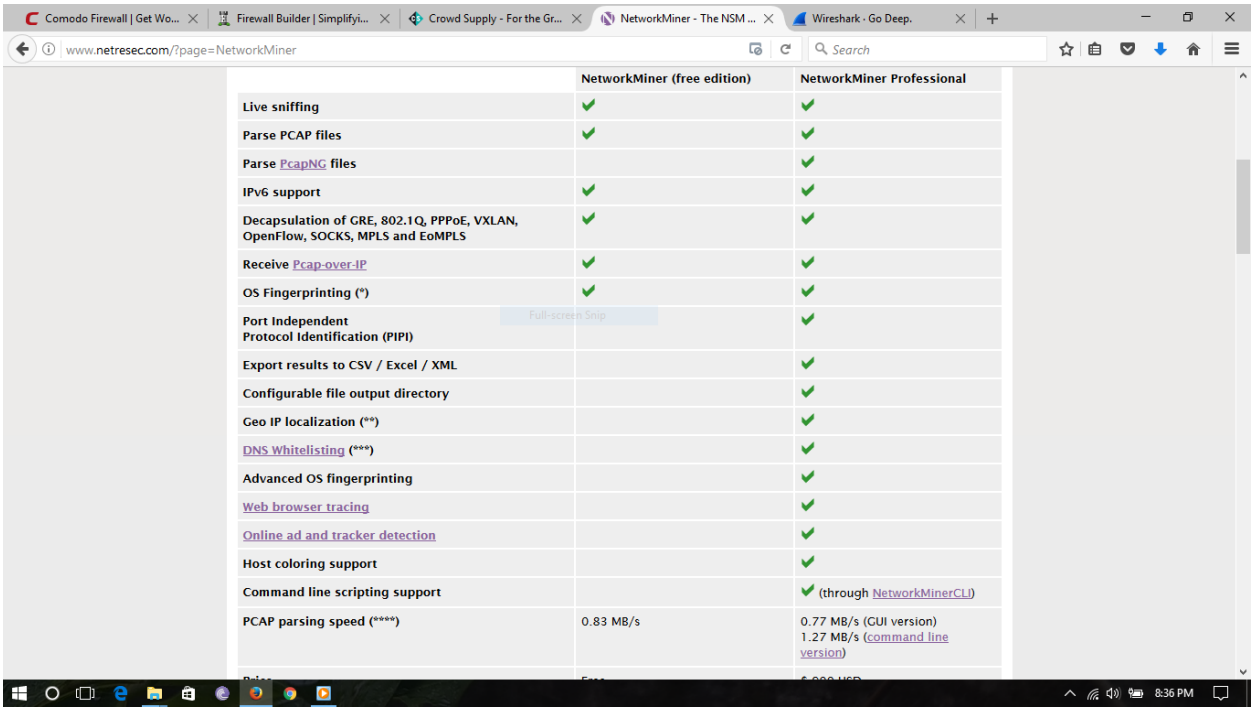
Logic

and or &&	Logical AND
or or ||	Logical OR
xor or ^^	Logical XOR
not or !	Logical NOT
[n] [...]	Substring operator

Tools:

NetworkMiner





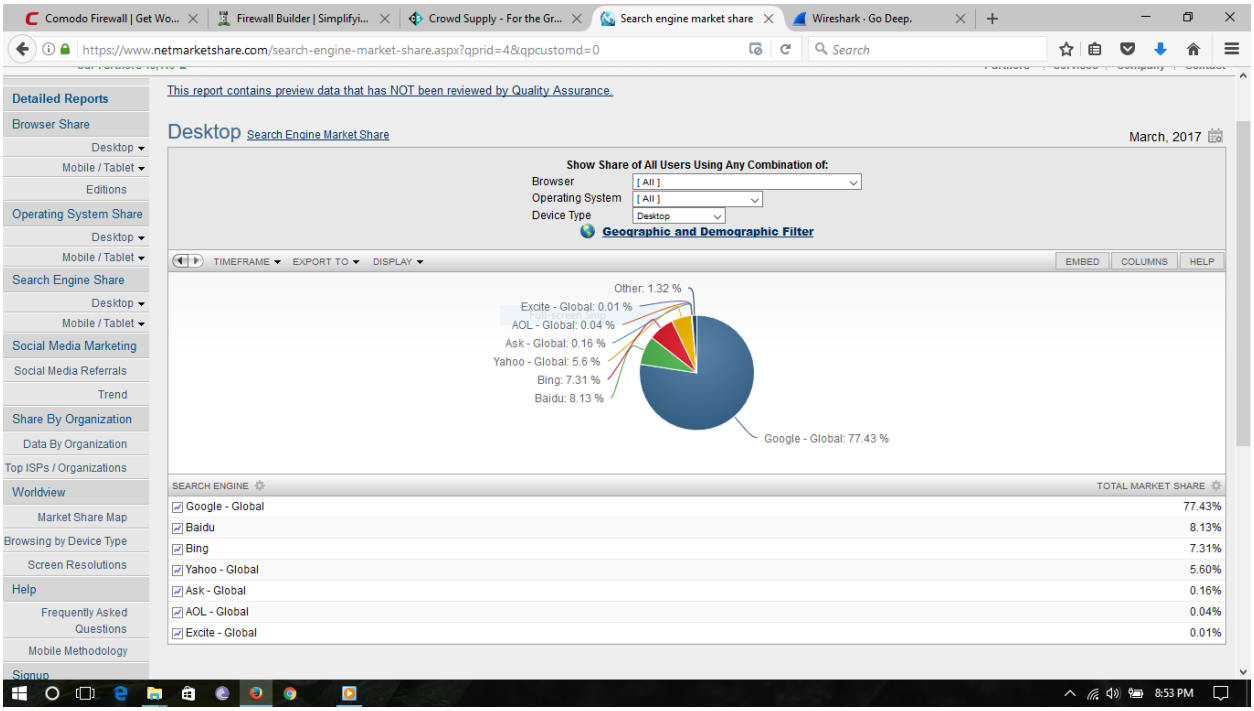
WinPcap


Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
Crowd Supply - For the Gr...
WinPcap - Download
Wireshark · Go Deep.
https://www.winpcap.org/install/default.htm
Search
WinPcap
The industry-standard windows packet capture library
WinPcap
WinDump
NTAR
Search
AirPcap
Powerful WiFi Capture Adapter for Windows
802.11 a/b/g/n compatible capture and injection, optimized for Wireshark
Download WinPcap for Windows
The latest stable WinPcap version is 4.1.3
At the moment there is no development version of WinPcap. For the list of changes, refer to the changelog.
Version 4.1.3 Installer for Windows
Driver +DLLs
Supported platforms:
Windows NT4/2000
Windows XP/2003/Vista/2008/Win7/2008R2/Win8 (x86 and x64)
Download
Get WinPcap
MD5 Checksum: a11a2f0cfe6d0b4c50945989db6360cd
SHA1 Checksum: e2516fcd1573e70334c8f50bee5241cdfdf48a00
This executable file installs WinPcap on your machine.
Instructions
1. Download and run the executable
2. Follow the instructions on the screen. The installation applet will automatically detect the operating system and install the correct drivers
3. The WinPcap-based applications are now ready to work
4. To remove WinPcap from the system, go to the Control Panel, click on "Add/Remove programs" and then select "WinPcap"
WinPcap Enhancements
AirPcap®: 802.11 Wireless Packet Capture Device
View management, control and data frames in Wireshark
Plug & play 802.11 a/b/g/n capture
Multi-channel aggregation
USB form factor
Learn More
TurboCap Gigabit Capture Card
Full-speed GigE capture and injection
Port aggregation
Pass-thru mode
Aggregating tap
Exported interfaces
TurboCap API developer's pack
Sample applications like "dump-to-disk" for high-speed capture to
8:33 PM

How We Are Tracked Online

- Operating systems
- Applications
- Security applications
- Application designed to track
- Malware
- Network devices
- DNS
- Auto update
- Any automatic connections
- Error reports
- Login
- Sites visited
- 3rd party sites
- Ad networks
- Email provider
- Internet service provider
- Cell provider
- Governments

Search Engines and Privacy



How Google uses pattern recognition

How Google uses pattern recognition to make sense of images

Computers don't "see" photos and videos in the same way that people do. When you look at a photo, you might see your best friend standing in front of her house. From a computer's perspective, that same image is simply a bunch of data that it may interpret as shapes and information about color values. While a computer won't react like you do when you see that photo, a computer can be trained to recognize certain patterns of color and shapes. For example, a computer might be trained to recognize the common patterns of shapes and colors that make up a digital image of a face. This process is known as facial detection, and it's the technology that helps Google to protect your privacy on services like Street View, where computers try to detect and then blur the faces of any people that may have been standing on the street as the Street View car drove by. It is also what helps services like Google+ photos suggest that you tag a photo or video, since it seems like there might be a face present. Facial detection won't tell you whose face it is, but it can help to find the faces in your photos.

If you get a little more advanced, the same pattern recognition technology that powers facial detection can help a computer to understand characteristics of the face it has detected. For example, there might be certain patterns that suggest a face is wearing a beard or glasses, or that it has attributes like those.

Information like this can be used to help with features like red-eye reduction or can let you lighten things up by placing a mustache or a monocle in the right place on your face when you are in a Hangout.

Beyond facial detection technology, Google also uses facial recognition in certain features. Facial recognition, like the name suggests, can help a computer to compare known faces against a new face and see if there is a probable match or similarity.

Advertising

Advertising keeps Google and many of the websites and services you use free of charge. We work hard to make sure that ads are safe, unobtrusive, and as relevant as possible. For example, you won't see pop-up ads on Google, and we terminate the accounts of hundreds of thousands of publishers and advertisers that violate our policies each year – including ads containing malware, ads for counterfeit goods, or ads that attempt to misuse your personal information.

How Google uses cookies in advertising

Cookies help to make advertising more effective. Without cookies, it's harder for an advertiser to reach its audience, or to know how many ads were shown and how many clicks they received.

Many websites, such as news sites and blogs, partner with Google to show ads to their visitors. Working with our partners, we may use cookies for a number of purposes, such as to stop you from seeing the same ad over and over again, to detect and stop click fraud, and to show ads that are likely to be more relevant (such as ads based on websites you have visited).

We store a record of the ads we serve in our logs. These server logs typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. We store this data for a number of reasons, the most important of which are to improve our services and to maintain the security of our systems. We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months).

Google keeps your searches and other identifiable user information for an undefined period of time Discussion

Google collects a lot of information about the services you use and how you use them, including when you visit a website using a Google service for advertisement. In the past, Google stated in their Privacy Policy: “We strike a reasonable balance between the competing pressures we face, such as the privacy of our users, the security of our systems and the need for innovation. We believe anonymizing IP addresses after 9 months and cookies in our search engine logs after 18 months strikes the right balance”. Today, these limitations of time are gone from the Privacy Policy, although some pages still acknowledge this. So we must conclude that Google has decided to stop trying to find the right balance between privacy of users and their own needs.

- Google can use your content for all their existing and future services Discussion

The content you post on a particular Google service can be used by Google on other services you may not be aware of.

- This service tracks you on other websites Discussion

This service uses cookies to track you even if you are not interacting with them directly. Amazon for instance, use cookies to track your device and serve targeted advertisements on other websites (Amazon associates, websites using Amazon Checkout). They “obtain certain types of information when your Web browser accesses Amazon.com or advertisements and other content served by or on behalf of Amazon.com on other Web sites”.

- Google can share your personal information with other parties Discussion

Google can share your personal information with other parties. For sensitive information (medical, racial, ethnic, political, religious or sexuality) Google requires “opt-in”. Google can also share or publish aggregated data that does not identify a person

- Google may stop providing services to you at any time Discussion

“Google may also stop providing Services to you, or add or create new limits to our Services at any time.” Google has no obligation from the terms to give you notice in advance or to give a reason for that termination

+ Limited copyright license to operate and improve all Google Services Discussion

The copyright license you grant is “for the limited purpose of operating, promoting, and improving” existing and new Google Services. However, please note that the license does not end if you stop using the Google services.

+ Google enables you to get your information out when a service is discontinued Discussion

Google gives you reasonable advance notice when a service is discontinued and “a chance to get information out of that Service.”

+ Google posts notice of changes, with a 14-day ultimatum. Discussion

Google “will post notice of modifications to these terms on this page. [They] will post notice of modified additional terms in the applicable Service. Changes will not apply retroactively and will become effective no sooner than fourteen days after they are posted.” As far as changes to the privacy policy goes: “We will not reduce your rights under this Privacy Policy without your explicit consent.” and if changes are significant Google will email you for some services.

- Google keeps the rights on your content when you stop using it Discussion

The license that you grant to Google on content you upload to their services will continue even if you stop using the services. While this makes sense for some services (e.g. Google Maps) this applies by default to all Google services. Otherwise you need to check each service for ways to remove content and for specific clauses that restrict the license in time.

+ Partial archives of their terms are available Discussion

At http://www.google.com/intl/en/policies/terms/archive/ you can see at least one previous versions of Google's terms

· Jurisdiction in California Discussion

“The laws of California, U.S.A., excluding California’s conflict of laws rules, will apply to any disputes arising out of or relating to these terms or the Services.All claims arising out of or relating to these terms or the Services will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.”

Types of location data used by Google

Different types of location information may be used in various Google products.

Implicit location information is information that does not actually tell us where your device is located, but allows us to infer that you are either interested in the place or that you might be at the place. An example of implicit location information would be a manually typed search query for a particular place. Implicit location information is used in a variety of ways. For example, if you type in “Eiffel Tower”, we infer that you may like to see information for places near Paris, and we can then use that to provide recommendations about those local places to you.

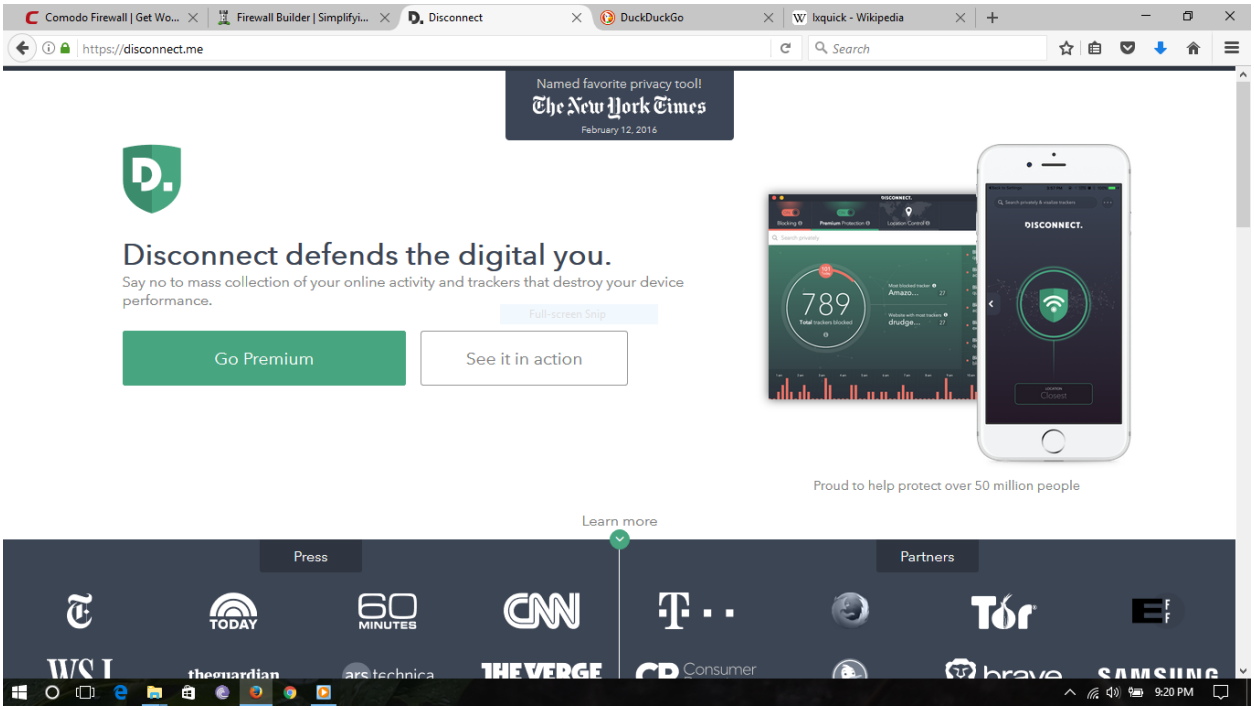
Internet traffic information, such as IP address, is usually assigned in country-based blocks, so it can be used to at least identify the country of your device, and do things such as to provide you with the correct language and locale for search queries. This information is sent as a normal part of internet traffic.

Some products, such as turn-by-turn navigation in Google Maps for mobile, use more precise location information. For these products, you typically have to choose to turn on device-based location services, which are services that use information such as GPS signals, device sensors, Wi-Fi access points, and cell tower ids that can be used to derive or estimate precise location. You can subsequently choose to turn the device-based location services off. Certain devices and/or applications might also offer you

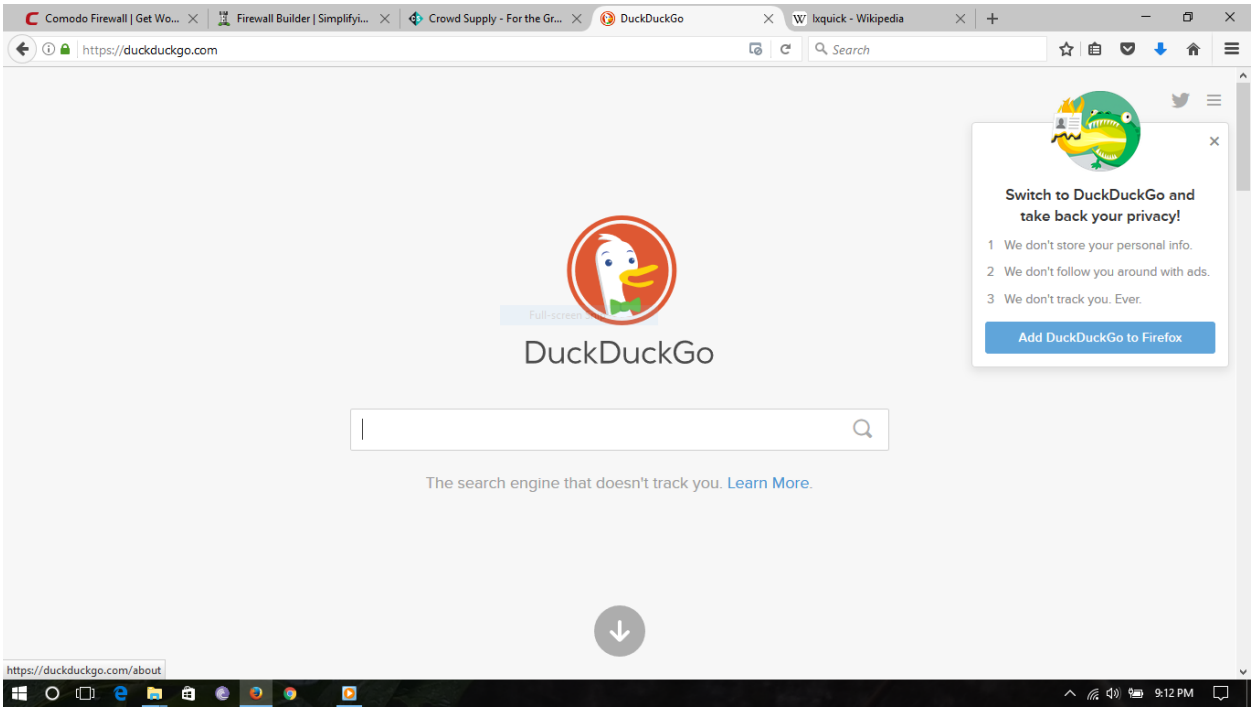
additional location control settings for these device-based location services. For example, in some products, you can choose whether to store these locations in that product or account's history.

Private searching:

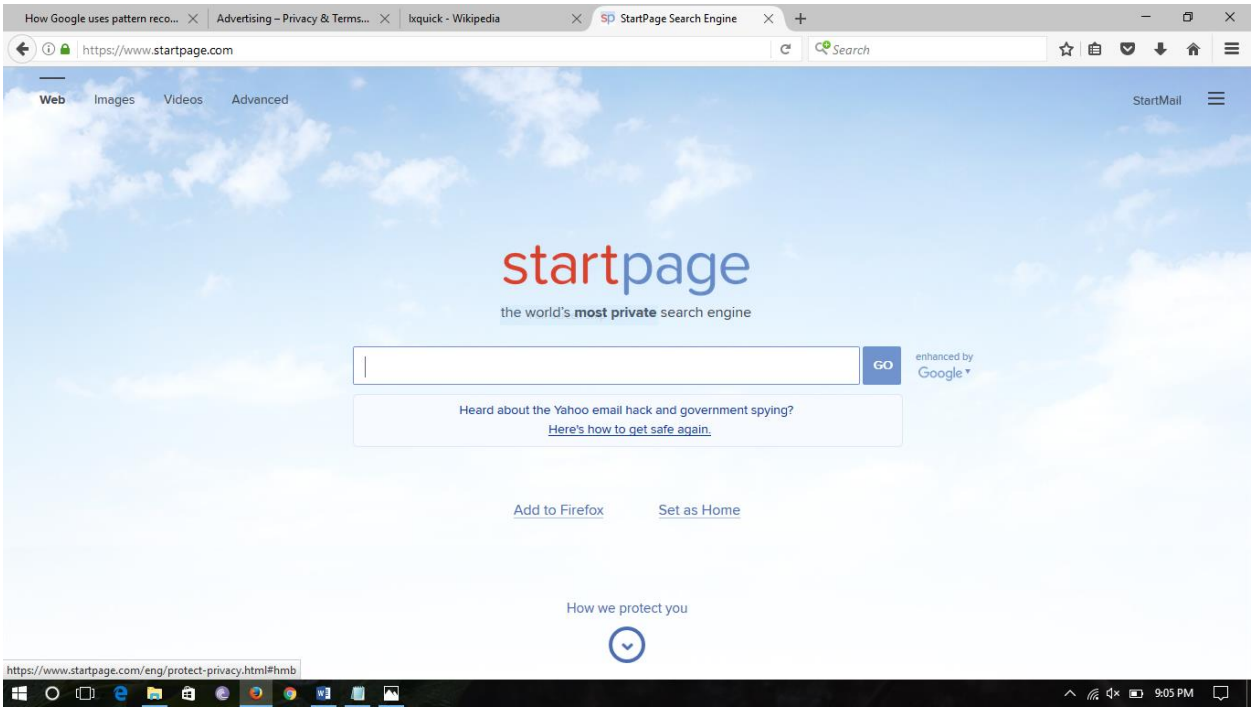
Disconnect



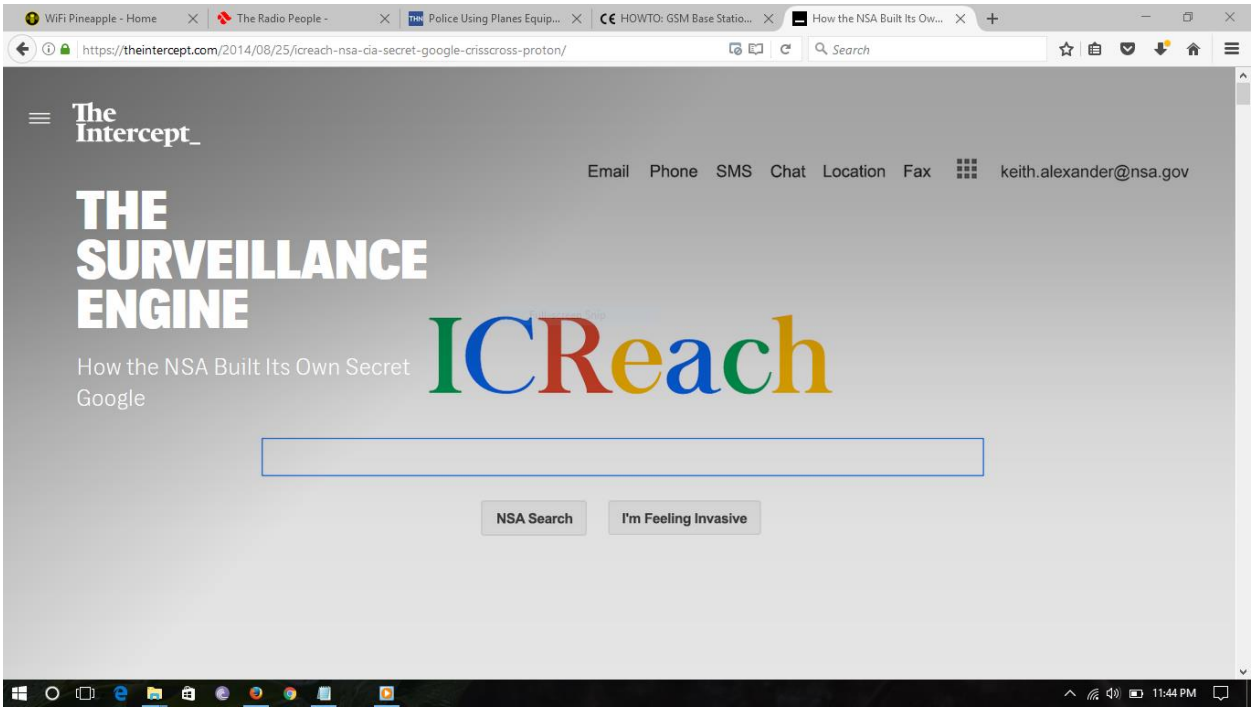
DuckDuckGo



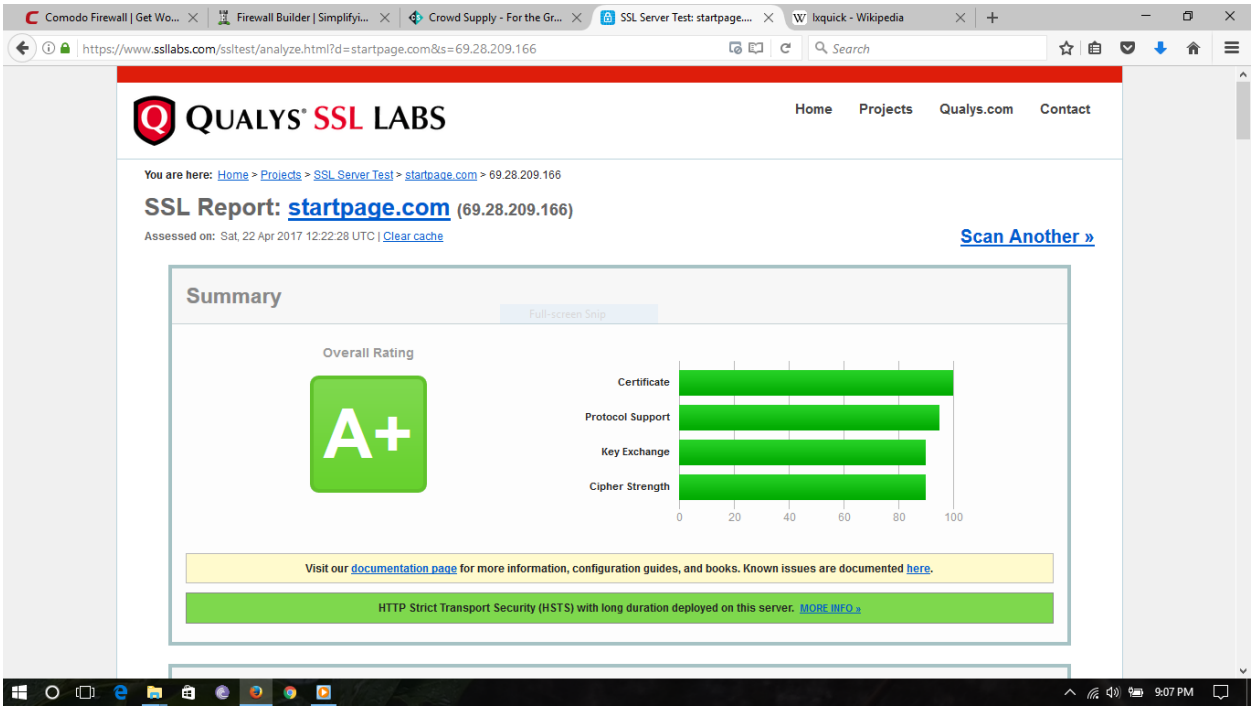
Ixquick(startpage)

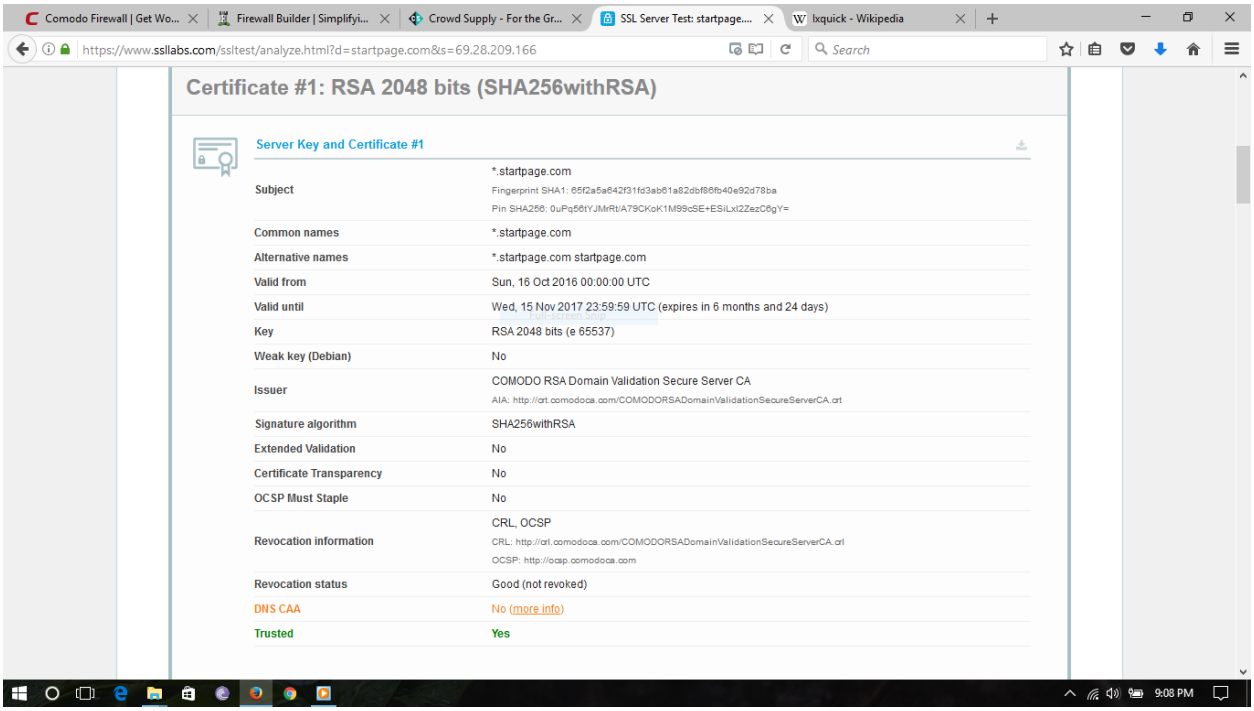


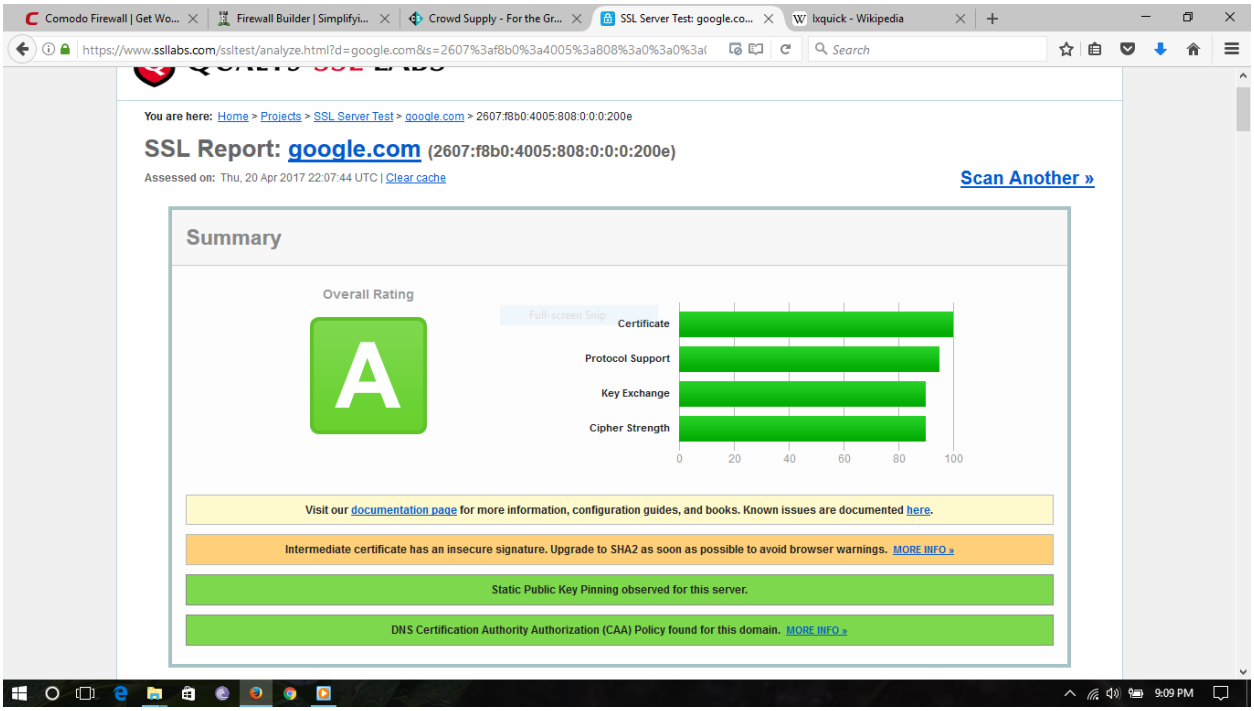
NSA Top secret search engine

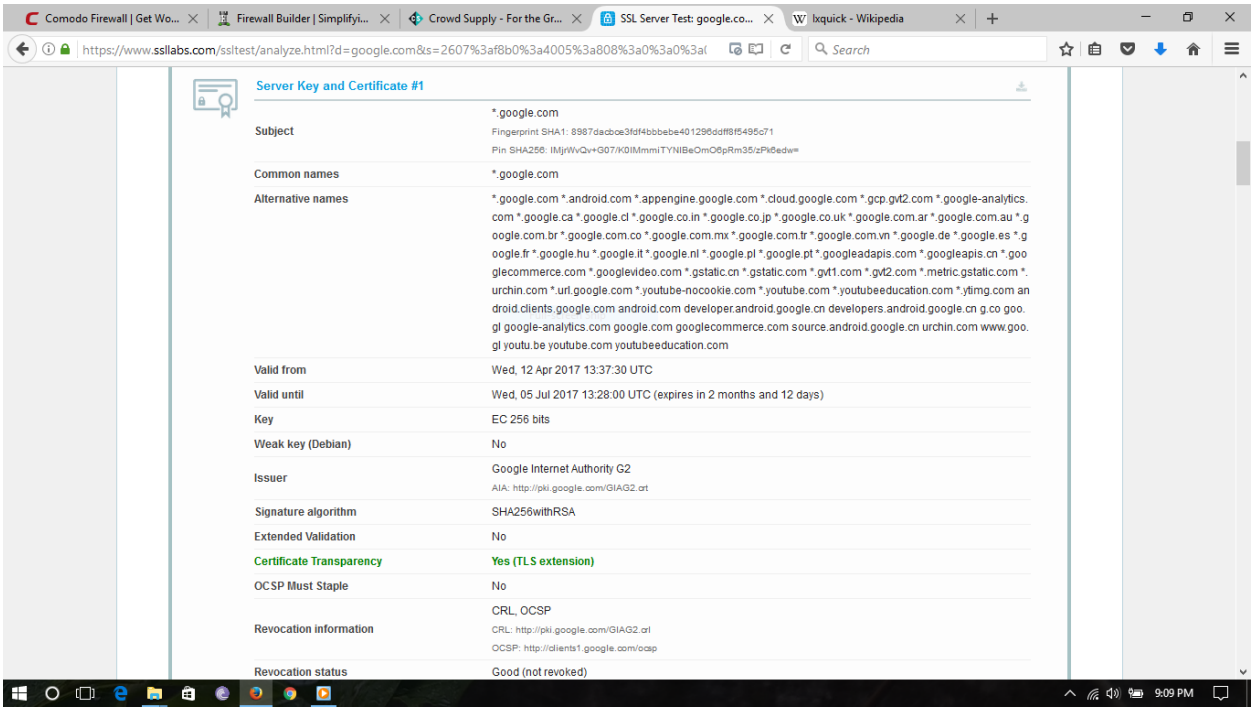


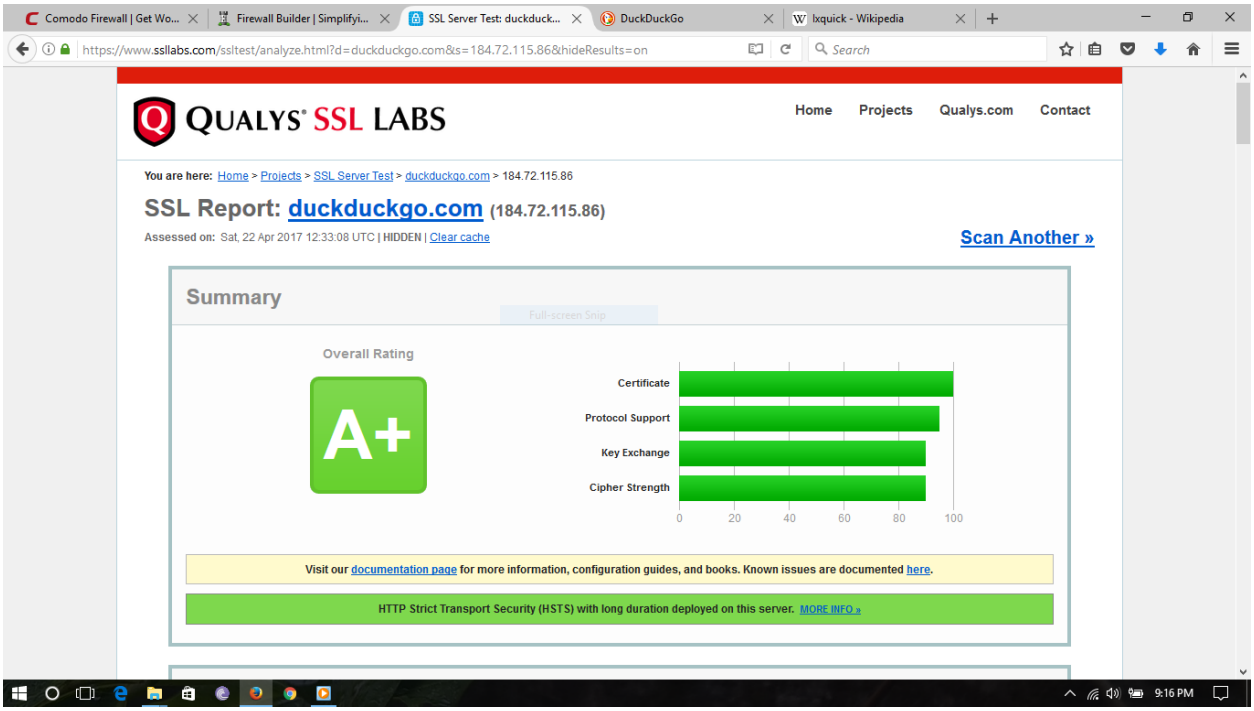
SSLLABS Ratings:

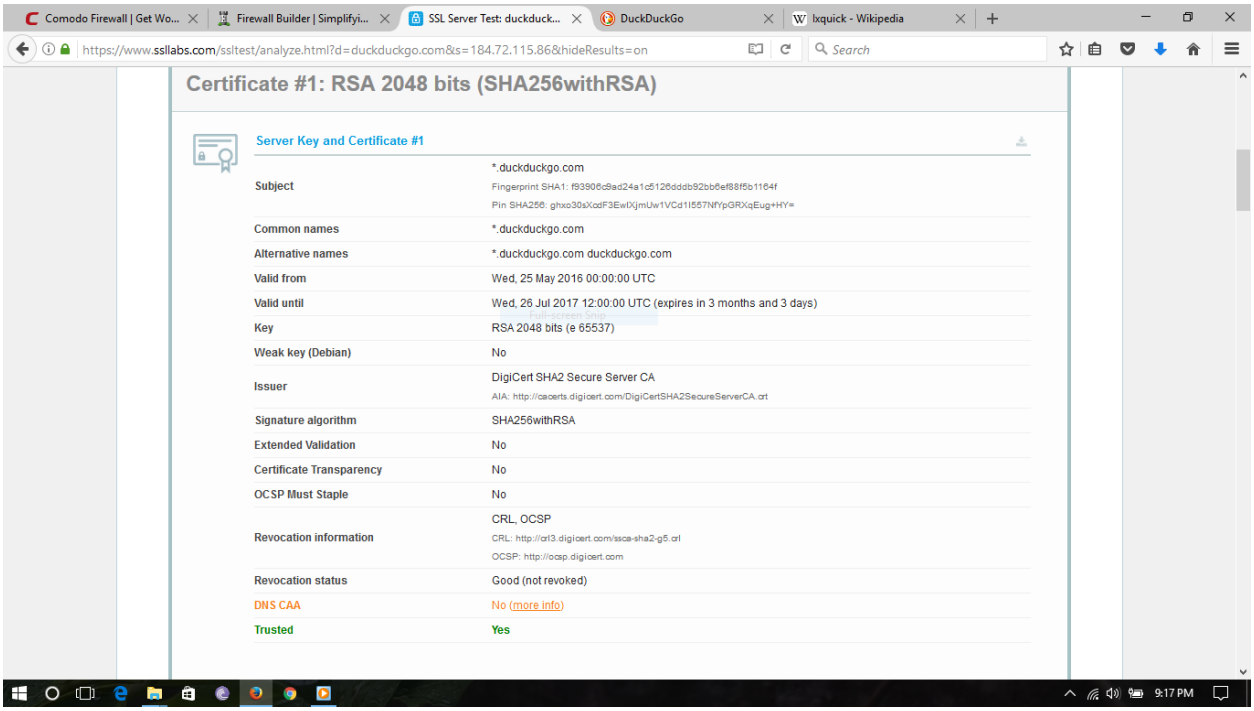


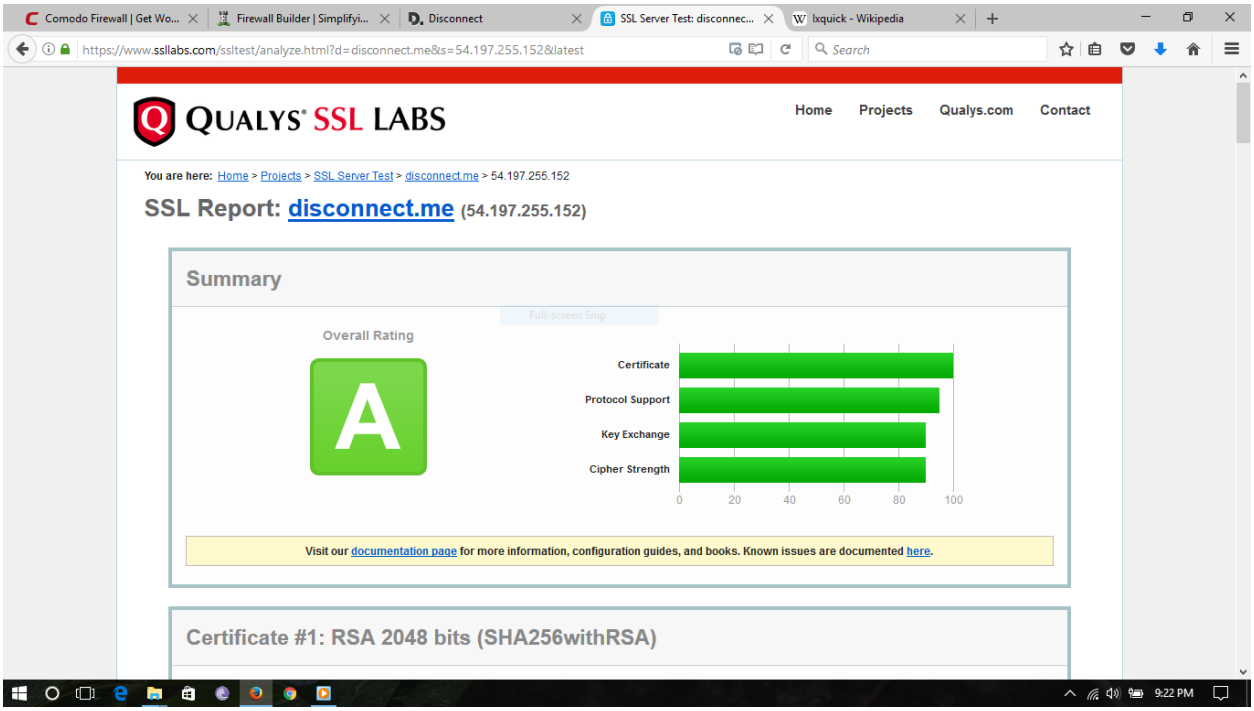


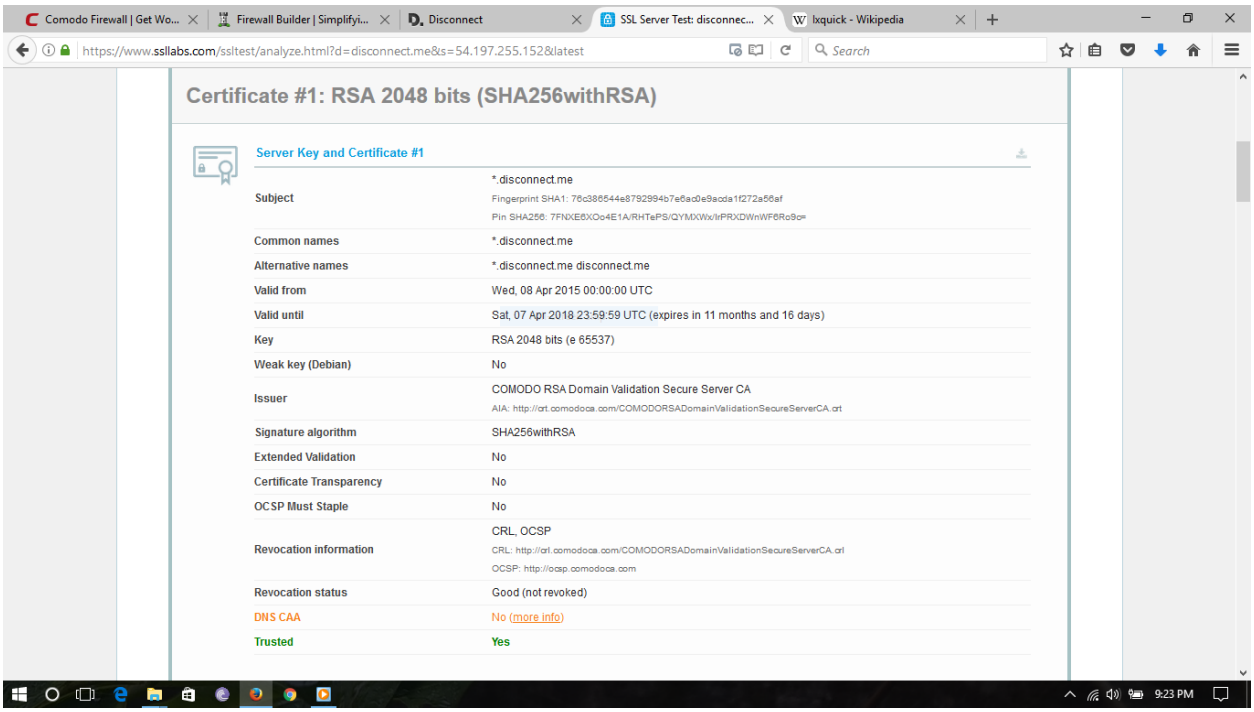

Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
Crowd Supply - For the Gr...
SSL Server Test: google.co...
lxquick - Wikipedia
https://www.ssllabs.com/ssltest/analyze.html?d=google.com&s=2607%3af8b0%3a4005%3a808%3a0%3a0%3a0
Search
You are here: Home > Projects > SSL Server Test > google.com > 2607:f8b0:4005:808:0:0:0:200e
SSL Report: google.com (2607:f8b0:4005:808:0:0:0:200e)
Assessed on: Thu, 20 Apr 2017 22:07:44 UTC | Clear cache
Scan Another »
Summary
Overall Rating
A
Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.
Intermediate certificate has an insecure signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. MORE INFO »
Static Public Key Pinning observed for this server.
DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »
9:09 PM


Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
Crowd Supply - For the Gr...
SSL Server Test: google.co...
lxquick - Wikipedia
https://www.ssllabs.com/ssltest/analyze.html?d=google.com&s=2607%3af8b0%3a4005%3a808%3a0%3a0%3a0
Search
Server Key and Certificate #1
Subject
*.google.com
Fingerprint SHA1: 8987dacbce3fdf4bbbebe401296ddff8f5495c71
Pin SHA256: IMjrWvQv+G07/K0IMmmiTYNIBeOmO6pRm35/zPk6edw=
Common names
*.google.com
Alternative names
*.google.com *.android.com *.appengine.google.com *.cloud.google.com *.gcp.gvt2.com *.google-analytics.com *.google.ca *.google.cl *.google.co.in *.google.co.jp *.google.co.uk *.google.com.ar *.google.com.au *.google.com.br *.google.com.co *.google.com.mx *.google.com.tr *.google.com.vn *.google.de *.google.es *.google.fr *.google.hu *.google.it *.google.nl *.google.pl *.google.pt *.googleadapis.com *.googleapis.cn *.googlecommerce.com *.googlevideo.com *.gstatic.cn *.gstatic.com *.gvt1.com *.gvt2.com *.metric.gstatic.com *.urchin.com *.url.google.com *.youtube-nocookie.com *.youtube.com *.youtubeeducation.com *.ytimg.com android.clients.google.com android.com developer.android.google.cn developers.android.google.cn g.co goo.gl google-analytics.com google.com googlecommerce.com source.android.google.cn urchin.com www.goo.gl youtu.be youtube.com youtubeeducation.com
Valid from
Wed, 12 Apr 2017 13:37:30 UTC
Valid until
Wed, 05 Jul 2017 13:28:00 UTC (expires in 2 months and 12 days)
Key
EC 256 bits
Weak key (Debian)
No
Issuer
Google Internet Authority G2
AIA: http://pki.google.com/GIAG2.crt
Signature algorithm
SHA256withRSA
Extended Validation
No
Certificate Transparency
Yes (TLS extension)
OCSP Must Staple
No
Revocation information
CRL, OCSP
CRL: http://pki.google.com/GIAG2.crl
OCSP: http://clients1.google.com/ocsp
Revocation status
Good (not revoked)
9:09 PM


Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
SSL Server Test: duckduck...
DuckDuckGo
lxquick - Wikipedia
https://www.ssllabs.com/ssltest/analyze.html?d=duckduckgo.com&s=184.72.115.86&hideResults=on
Search
QUALYS SSL LABS
Home
Projects
Qualys.com
Contact
You are here: Home > Projects > SSL Server Test > duckduckgo.com > 184.72.115.86
SSL Report: duckduckgo.com (184.72.115.86)
Assessed on: Sat, 22 Apr 2017 12:33:08 UTC | HIDDEN | Clear cache
Scan Another »
Summary
Overall Rating
A+
Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.
HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »
9:16 PM


Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
SSL Server Test: duckduck...
DuckDuckGo
lxquick - Wikipedia
https://www.ssllabs.com/ssltest/analyze.html?d=duckduckgo.com&s=184.72.115.86&hideResults=on
Search
Certificate #1: RSA 2048 bits (SHA256withRSA)
Server Key and Certificate #1
Subject
*.duckduckgo.com
Fingerprint SHA1: f93906c9ad24a1c5126dddb92bb6ef88f5b1164f
Pin SHA256: ghxo30sXcdF3EwIXjmUw1VCd1l557NfYpGRXqEug+HY=
Common names
*.duckduckgo.com
Alternative names
*.duckduckgo.com duckduckgo.com
Valid from
Wed, 25 May 2016 00:00:00 UTC
Valid until
Wed, 26 Jul 2017 12:00:00 UTC (expires in 3 months and 3 days)
Key
RSA 2048 bits (e 65537)
Weak key (Debian)
No
Issuer
DigiCert SHA2 Secure Server CA
AIA: http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt
Signature algorithm
SHA256withRSA
Extended Validation
No
Certificate Transparency
No
OCSP Must Staple
No
Revocation information
CRL, OCSP
CRL: http://crl3.digicert.com/ssca-sha2-g5.crl
OCSP: http://ocsp.digicert.com
Revocation status
Good (not revoked)
DNS CAA
No (more info)
Trusted
Yes
9:17 PM


Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
Disconnect
SSL Server Test: disconnec...
lxquick - Wikipedia
https://www.ssllabs.com/ssltest/analyze.html?d=disconnect.me&s=54.197.255.152&latest
Search
QUALYS SSL LABS
Home
Projects
Qualys.com
Contact
You are here: Home > Projects > SSL Server Test > disconnect.me > 54.197.255.152
SSL Report: disconnect.me (54.197.255.152)
Summary
Overall Rating
A
Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.
Certificate #1: RSA 2048 bits (SHA256withRSA)
9:22 PM


Comodo Firewall | Get Wo...
Firewall Builder | Simplifyi...
Disconnect
SSL Server Test: disconnec...
lxquick - Wikipedia
https://www.ssllabs.com/ssltest/analyze.html?d=disconnect.me&s=54.197.255.152&latest
Search
Certificate #1: RSA 2048 bits (SHA256withRSA)
Server Key and Certificate #1
Subject
*.disconnect.me
Fingerprint SHA1: 76c386544e8792994b7e6ac0e9acda1f272a56af
Pin SHA256: 7FNXE6XOo4E1A/RHTePS/QYMXWx/IrPRXDWnWF6Ro9c=
Common names
*.disconnect.me
Alternative names
*.disconnect.me disconnect.me
Valid from
Wed, 08 Apr 2015 00:00:00 UTC
Valid until
Sat, 07 Apr 2018 23:59:59 UTC (expires in 11 months and 16 days)
Key
RSA 2048 bits (e 65537)
Weak key (Debian)
No
Issuer
COMODO RSA Domain Validation Secure Server CA
AIA: http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt
Signature algorithm
SHA256withRSA
Extended Validation
No
Certificate Transparency
No
OCSP Must Staple
No
Revocation information
CRL, OCSP
CRL: http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl
OCSP: http://ocsp.comodoca.com
Revocation status
Good (not revoked)
DNS CAA
No (more info)
Trusted
Yes
9:23 PM

Passwords and Authentication Methods

Pass the hash

In cryptanalysis and computer security, pass the hash is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying NTLM or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.

After an attacker obtains valid user name and user password hash values (somehow, using different methods and tools), they are then able to use that information to authenticate to a remote server or service using LM or NTLM authentication without the need to brute-force the hashes to obtain the cleartext password (as it was required before this technique was published). The attack exploits an implementation weakness in the authentication protocol, where password hash remain static from session to session until the password is next changed.

This technique can be performed against any server or service accepting LM or NTLM authentication, whether it runs on a machine with Windows, Unix, or any other operating system.

Dictionary Attack

The dictionary attack, or “straight mode,” is a very simple attack mode. It is also known as a “Wordlist attack”.

All that is needed is to read line by line from a textfile (aka “dictionary” or “wordlist”) and try each line as a password candidate.

Combinator Attack

Input

If dictionary contains the words:

```
pass
12345
omg
Test
```

Output

Hashcat creates the following password candidates:

```
passpass
pass12345
passomg
passTest
12345pass
1234512345
12345omg
12345Test
omgpass
omg12345
omgomg
omgTest
Testpass
Test12345
Testomg
TestTest
```

Using the Combinator Attack within hashcat (not standalone version of Combinator Attack).

The command for the Combinator Attack in hashcat is -a 1

Need to specify exactly 2 dictionaries in you command line: e.g.

```
./hashcat64.bin -m 0 -a 1 hash.txt dict1.txt dict2.txt
```

If wish to add rules to either the left or right dictionary or both at once then you can use the -j or -k commands.

```
-j,  --rule-left=RULE              Single rule applied to each word on the
left dictionary

-k,  --rule-right=RULE             Single rule applied to each word on the
right dictionary
```

Example.

Dictionary 1

```
yellow
green
black
blue
```

Dictionary 2

```
car
bike
```

Commands

-j '$-'

-k '$!'

Output:

```
yellow-car!
green-car!
black-car!
blue-car!
yellow-bike!
green-bike!
black-bike!
blue-bike!
```

Hybrid Attack

Basically, the hybrid attack is just a Combinator attack. One side is simply a dictionary, the other is the result of a Brute-Force attack. In other words, the full Brute-Force keyspace is either appended or prepended to each of the words from the dictionary. That's why it's called “hybrid”.

Alternatively you can use Mask attack or Rule-based attack to replace the Brute-Force side.

If your example.dict contains:

```
password
hello
```

The configuration:

```
$ ... -a 6 example.dict ?d?d?d?d
```

Generates the following password candidates:

```
password0000
password0001
password0002
.
.
.
password9999
hello0000
hello0001
hello0002
.
.
.
hello9999
```

It also works on the opposite side!

The configuration:

```
$ ... -a 7 ?d?d?d?d example.dict
```

Generates the following password candidates:

```
0000password
0001password
0002password
.
.
.
9999password
0000hello
0001hello
0002hello
.
.
.
9999hello
```

Mask Attack

For each position of the generated password candidates we need to configure a placeholder. If a password we want to crack has the length 8, our mask must consist of 8 placeholders.

- A mask is a simple string that configures the keyspace of the password candidate engine using placeholders.
- A placeholder can be either a custom charset variable, a built-in charset variable or a static letter.
- A variable is indicated by the ? letter followed by one of the built-in charset (l, u, d, s, a) or one of the custom charset variable names (1, 2, 3, 4).
- A static letter is not indicated by a letter. An exception is if we want the static letter ? itself, which must be written as ??.

Output

Optimized due its partially reverse algorithms, password candidates are generated in the following order:

```
aaaaaaaa
aaaabaaa
aaaacaaa
.
.
.
aaaaxzzz
aaaayzzz
aaaazzzz
```

```
baaaaaaa
baaabaaa
baaacaaa
.
.
.
baaaxzzz
baaayzzz
baaazzzz
.
.
.
zzzzzzzz
```

Built-in charsets

- ?l = abcdefghijklmnopqrstuvwxyz
- ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ?d = 0123456789
- ?s = «space»!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
- ?a = ?l?u?d?s
- ?b = 0x00 - 0xff

Custom charsets

All hashcat derivates have four commandline-parameters to configure four custom charsets.

```
--custom-charset1=CS
--custom-charset2=CS
--custom-charset3=CS
--custom-charset4=CS
```

Password length increment

A Mask attack is always specific to a password length. For example, if we use the mask “?l?l?l?l?l?l?l?l” we can only crack a password of the length 8. But if the password we try to crack has the length 7 we will not find it. Thats why we have to repeat the attack several times, each time with one placeholder added to the mask. This is transparently automated by using the “--increment” flag (Attention: the mask length itself is the limiting factor for hashcat. That implies that if i.e. the mask is only of length 4 --increment won't increment the length of the password candidates above 4. A mask of length, therefore, won't increase at all even if --increment was specified).

```
?l
?l?l
?l?l?l
?l?l?l?l
?l?l?l?l?l
?l?l?l?l?l?l
?l?l?l?l?l?l?l
?l?l?l?l?l?l?l?l
```

Hashcat charset files

Hashcat charsets files (file extension: .hcchr) are a convenient way to reuse charsets, define custom charsets and use the language-specific charsets shipped by hashcat.

These files can be used together with the --custom-charsetN= (or -1, -2, -3 and -4) parameter. Instead of providing all the charset directly on command line, the support for .hcchr files allows one to specify the path to the file:

```
-1 charsets/standard/German/de_cp1252.hcchr
```

It is important that .hcchr files are created with language specific file encodings (e.g. cp1252, ISO-8859-15 etc). For examples of content and encoding of .hcchr files, see the examples shipped with hashcat (e.g. [HASHCATROOT]/charsets/standard/Italian/).

Hashcat mask files

Hashcat mask files (file extension: .hcmask) are files which contain custom charsets (optional) and masks (e.g. ?1?1?1?1?d?d) line-by-line. The advantage of using .hcmask files, which are plain text files, is that those files allow the hashcat user to have a set of predefined and well-working masks stored within a file (or several e.g. password policy specific files) where the lines contained in the hcmask file could for instance be sorted by increasing runtime and/or likelihood of matches.

The general format of 1 single line in the .hcmask file is as follows:

```
[?1,][?2,][?3,][?4,]mask
```

Where the placeholders are as follows:

- [?1] the 1st custom charset (--custom-charset1 or -1) will be set to this value, optional
- [?2] the 2nd custom charset (--custom-charset2 or -2) will be set to this value, optional
- [?3] the 3rd custom charset (--custom-charset3 or -3) will be set to this value, optional
- [?4] the 4th custom charset (--custom-charset4 or -4) will be set to this value, optional
- [mask] the mask which should (but does not need) to use the custom-charset defined by [?1], [?2], [?3] or [?4] and can use any additional predefined charset (?d, ?l, ?u, ?s, ?a, ?b) and can contain fixed chars too (example value: pass?1?d?d?2?l?l)

Rule-based Attack

The rule-based attack is one of the most complicated of all the attack modes. The reason for this is very simple. The rule-based attack is like a programming language designed for password candidate generation. It has functions to modify, cut or extend words and has conditional operators to skip some, etc. That makes it the most flexible, accurate and efficient attack.

The following functions are 100% compatible to John the Ripper and PasswordsPro:

Name	Function	Description	Example Rule	Input Word	Output Word	Note
Nothing	:	do nothing	:	p@ssW0rd	p@ssW0rd	
Lowercase	l	Lowercase all letters	l	p@ssW0rd	p@ssw0rd	
Uppercase	u	Uppercase all letters	u	p@ssW0rd	P@SSW0RD	
Capitalize	c	Capitalize the first letter and lower the rest	c	p@ssW0rd	P@ssw0rd	
Invert Capitalize	C	Lowercase first found character, uppercase the rest	C	p@ssW0rd	p@SSW0RD	
Toggle Case	t	Toggle the case of all characters in word.	t	p@ssW0rd	P@SSw0RD	
Toggle @	TN	Toggle the case of characters at position N	T3	p@ssW0rd	p@sSW0rd	*
Reverse	r	Reverse the entire word	r	p@ssW0rd	dr0Wss@p	
Duplicate	d	Duplicate entire word	d	p@ssW0rd	p@ssW0rdp@ssW0rd	
Duplicate N	pN	Append duplicated word N times	p2	p@ssW0rd	p@ssW0rdp@ssW0rdp@ssW0rd	
Reflect	f	Duplicate word reversed	f	p@ssW0rd	p@ssW0rddr0Wss@p	

Name	Function	Description	Example Rule	Input Word	Output Word	Note
Rotate Left	{	Rotates the word left.	{	p@ssW0rd	@ssW0rdp	
Rotate Right	}	Rotates the word right	}	p@ssW0rd	dp@ssW0r	
Append Character	$X	Append character X to end	$1	p@ssW0rd	p@ssW0rd1	
Prepend Character	^X	Prepend character X to front	^1	p@ssW0rd	1p@ssW0rd	
Truncate left	[	Deletes first character	[	p@ssW0rd	@ssW0rd	
Trucate right	]	Deletes last character	]	p@ssW0rd	p@assW0r	
Delete @ N	DN	Deletes character at position N	D3	p@ssW0rd	p@sW0rd	*
Extract range	xNM	Extracts M characters, starting at position N	x04	p@ssW0rd	p@ss	* #
Omit range	ONM	Deletes M characters, starting at position N	O12	p@ssW0rd	psW0rd	*
Insert @ N	iNX	Inserts character X at position N	i4!	p@ssW0rd	p@ss!W0rd	*
Overwrite @ N	oNX	Overwrites character at position N with X	o3$	p@ssW0rd	p@s$W0rd	*
Truncate @ N	'N	Truncate word at position N	'6	p@ssW0rd	p@ssW0	

Name	Function	Description	Example Rule	Input Word	Output Word	Note
Replace	sXY	Replace all instances of X with Y	ss$	p@ssW0rd	p@$$W0rd	
Purge	@X	Purge all instances of X	@s	p@ssW0rd	p@W0rd	+
Duplicate first N	zN	Duplicates first character N times	z2	p@ssW0rd	ppp@ssW0rd	
Duplicate last N	ZN	Duplicates last character N times	Z2	p@ssW0rd	p@ssW0rddd	
Duplicate all	q	Duplicate every character	q	p@ssW0rd	pp@@ssssWW00rrdd	
Extract memory	XNMI	Insert substring of length M starting from position N of word saved to memory at position I	lMX428	p@ssW0rd	p@ssw0rdw0	+
Append memory	4	Append the word saved to memory to current word	uMl4	p@ssW0rd	p@ssw0rdP@SSW0RD	+
Prepend memory	6	Prepend the word saved to memory to current word	rMr6	p@ssW0rd	dr0Wss@pp@ssW0rd	+
Memorize	M	Memorize current word	lMuX084	p@ssW0rd	P@SSp@ssw0rdW0RD	+

- Indicates that N starts at 0. For character positions other than 0-9 use A-Z (A=10)
- + Indicates that this rule is implemented in hashcat only.
- # Changed in oclHashcat v1.37 → v1.38 and hashcat v0.51 → v0.52

Random rules

This is a very unique hashcat feature. With hashcat you can generate random rules on the fly to be used for that session. This is a good thing if you are out of ideas on what to do next when you have already tried all your rules on all your dictionaries. There are three configuration parameters:

Tells hashcat to generate NUM rules to be applied to each attempt:

```
--generate-rules=NUM
```

Specifies the number of functions that should be used (minimum to maximum range):

```
--generate-rules-func-min=NUM
--generate-rules-func-max=NUM
```

This number can be unlimited but large numbers are not recommended. When used in conjunction with –g, any rule outside of this setting will be ignored.

For example, it could randomly generate the rules “l r”, “l ^f”, and “sa@”, these are all valid rules to be used. However, “l ^f sa@ r $3” would be ignored as it contains 5 functions. Default: min=1 max=4

Saving matched rules

This becomes handy especially in combination with the rules generator but also for statistical analysis of your rule sets.

To save any rule that generated a matched password use these switches:

```
--debug-mode=1 --debug-file=matched.rule
```

This will save the matched rule on every match, so the resulting rule file might contain many duplicate rules.

Debugging rules

With hashcat we can debug our rules easily. That means we can verify that the rule we wrote actually does what we want it to do. All you need to use is the --stdout switch and omit the hashlist.

Here is an example:

Create simple dictionary:

```
$ echo WORd > word
```

Generate a simple rule. The “c” rule capitalizes the first letter and lower-cases the rest.

```
$ echo c > rule
```

And thats how we see the generated debug output:

```
$ ./hashcat-cli64.bin -r rule --stdout word
Word
```

This “feature” is also a very fast password candidate generator. That means that if we have some external program that supports reading from stdin we can feed it with our output.

Toggle-Case Attack

For each word in a dictionary, all possible combinations of upper- and lower-case variants are generated.

In hashcat-legacy, this attack was implemented as a stand-alone attack mode. In hashcat, we emulate this attack with a much more efficient ruleset.

The information for this section has moved to the Using rules to emulate toggle attack article.

Input

If our dictionary contains the word

```
pass1234
```

Output

Hashcat creates the following password candidates

```
pass1234
Pass1234
pAss1234
PAss1234
paSs1234
PaSs1234
pASs1234
PASs1234
pasS1234
PasS1234
pAsS1234
PAsS1234
paSS1234
PaSS1234
pASS1234
PASS1234
```

Hashdumps and Passwords

2010:			
Gawker	gawker-hashes	DES	690526 of 743855 (92%) done
2011:			
Project Mayhem	mayhem-hashes	MD5	76508 of 130884 (58%) done
Stratfor	stratfor-hashes	MD5	806179 of 860149 (93%) done
Rootkit.com	rootkit-hashes	MD5	69160 of 71228 (95%) done
2012:			
BKAV	bkav-encode-1	VB > 3.8.5	25019 of 113224 (22%) done
BKAV	bkav-encode-2	VB < 3.8.5	11210 of 20988 (53%) done
Project Blackstar	blackstar-encode-1	MD5	2469 of 3555 (68%) done
Project Blackstar	blackstar-1-2md5	2xMD5**	90 of 90 (100%) done
Project Blackstar	blackstar-encode-2	SHA1	1921 of 2389 (80%) done
Project Blackstar	blackstar-encode-3	MYSQL	4177 of 4262 (98%) done
LinkedIn	masked-150	SHA1**	3318770 of 3487579 (95%) done
LinkedIn	unmasked-100	SHA1	2286752 of 2936840 (77%) done

Gamigo	gamigo-hashes	MD5	6897480 of 7004341 (98%) done
EHarmony	eharmony-hashes	MD5	1476823 of 1516834 (97%) done
Project OpIsrael	opisrael-hashes	MD5	9816 of 10809 (90%) done
Project OpIsrael	opisrael-hashed-2md5	2xMD5**	3016 of 3016 (100%) done
Project Hellfire	hellfire-md5-hashes	MD5	19427 of 19988 (97%) done
Project Whitefox	whitefox-md5	MD5	44163 of 47238 (93%) done
InfoSecWest 2012	isw-2012-hash	MD5	114940455 of 139444502 (82%) don
InsidePro 2012	insidepro-2012-hash	MD5	28752887 of 29013076 (99%) done
2013:			
Project Sunrise	sunrise-hashes	MD5	7512 of 7660 (98%) done
Walla	walla-hashes	PHPBB	68183 of 256381 (26%) done
Casio.cn	casio-hashes	MD5	18297 of 24035 (76%) done
ABC	abc-hashes	SHA1	46414 of 49567 (93%) done
DamnSmallLinux	dsl-hashes	MD5	5562 of 14144 (39%) done

Dhool	dhool-hashes	MD5	14367 of 15302 (93%) done
Gaming	gaming-hashes	MD5	44791 of 50853 (88%) done
FFGBeach	ffgbeach-hashes	MD5	476266 of 481377 (99%) done
Battlefield	battlefield-hashes	MD5	541019 of 548686 (98%) done
OpNorthKorea	opnkorea-hashes	MD5	8978 of 9001 (99%) done
TomSawyer	tomsawyer-hashes	MD5	58518 of 61727 (94%) done
OpSea	opsea-hashes	MD5	4078 of 4151 (98%) done
Slyck	slyck-hashes	PHPBB	-
2014:			
Aha	aha-hashes	MD5	171029 of 180488 (94%) done
Forbes	forbes-hashes	PHPBB	-
Misc:			
Misc-pastebin-MD5 (click for "contributing" sites)	misc-pastebin-hashes	MD5	1650371 of 17865533 (9%) done

Password security

Hardware security module

A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server.

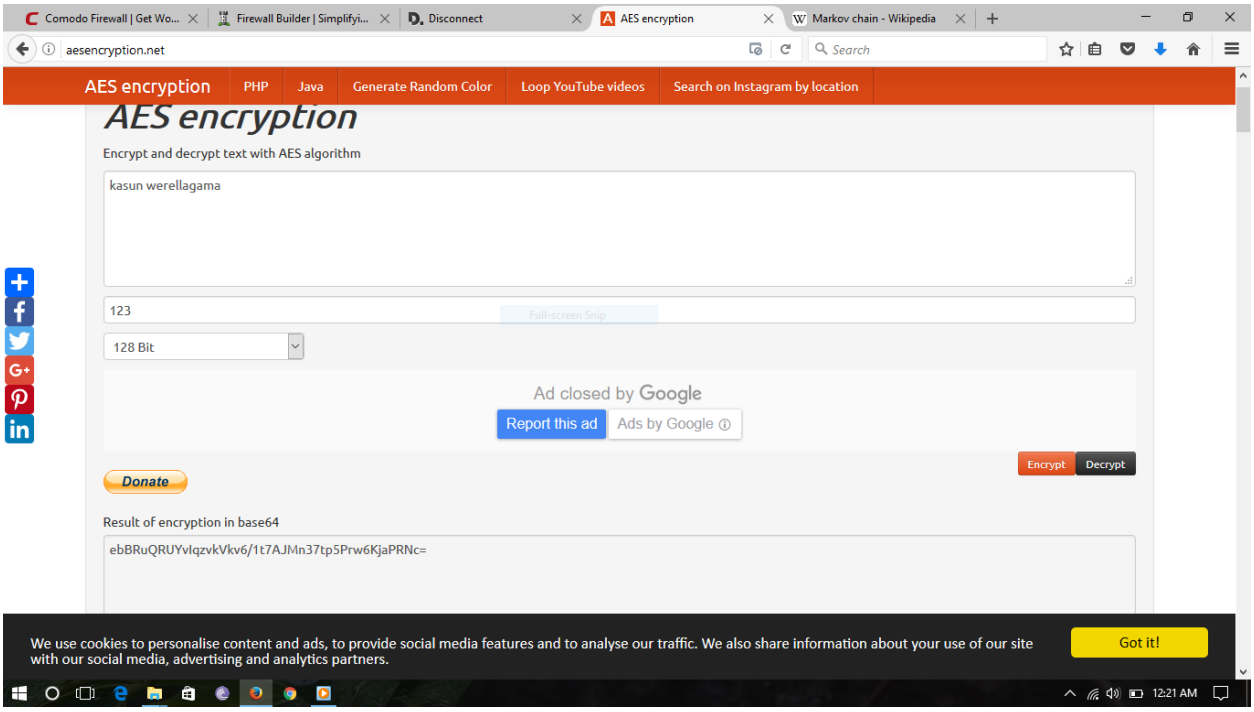
HSMs may possess controls that provide tamper evidence such as logging and alerting and tamper resistance such as deleting keys upon tamper detection. Each module contains one or more secure cryptoprocessor chips to prevent tampering and bus probing.

Many HSM systems have means to securely back up the keys they handle either in a wrapped form via the computer's operating system or externally using a smartcard or some other security token.

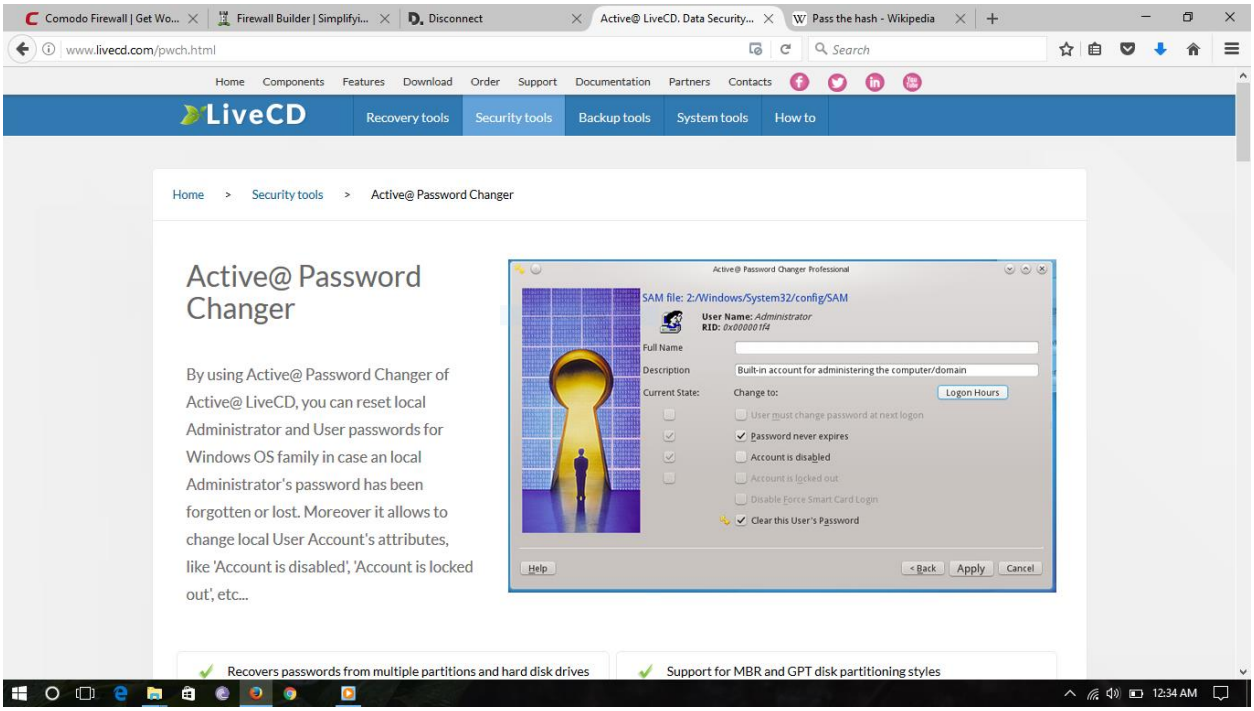
Because HSMs are often part of a mission-critical infrastructure such as a public key infrastructure or online banking application, HSMs can typically be clustered for high availability. Some HSMs feature dual power supplies and field replaceable components such as cooling fans to conform to the high-availability requirements of data center environments and to enable business continuity.

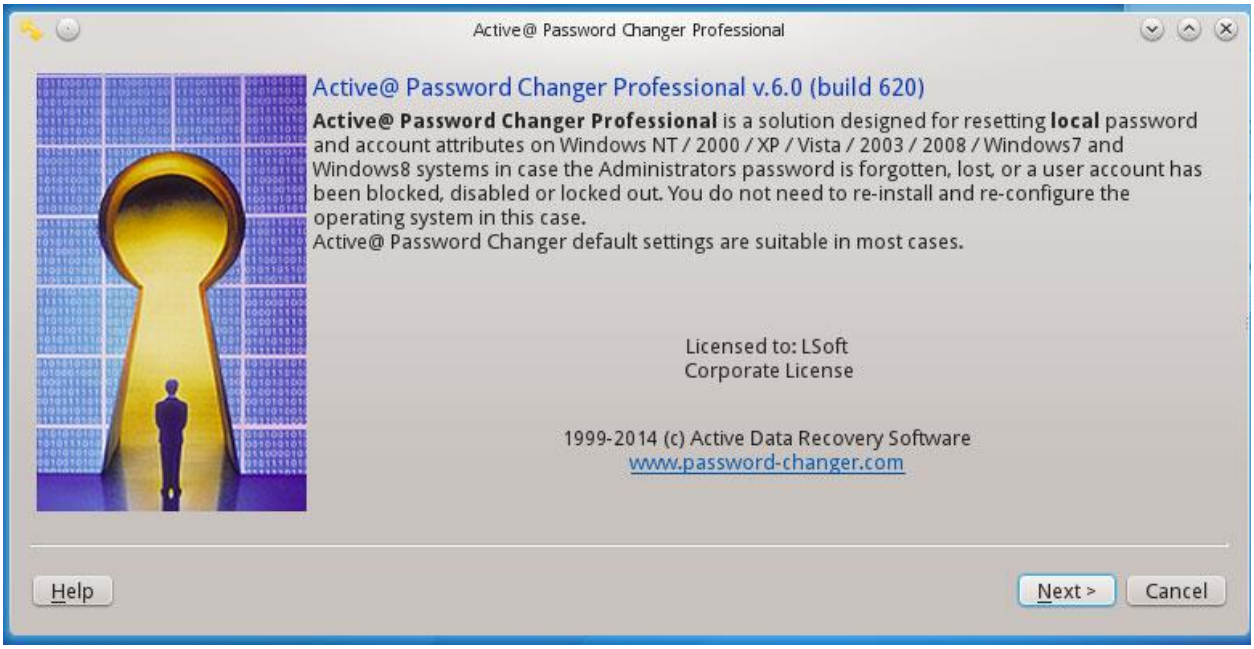
A few of the HSMs available in the market have the ability to execute specially developed modules within the HSM's secure enclosure. Such an ability is useful, for example, in cases where special algorithms or business logic has to be executed in a secured and controlled environment. The modules can be developed in native C language, in .NET, Java, or other programming languages. While providing the benefit of securing application-specific code, these execution engines protect the status of an HSM's FIPS or Common Criteria validation.

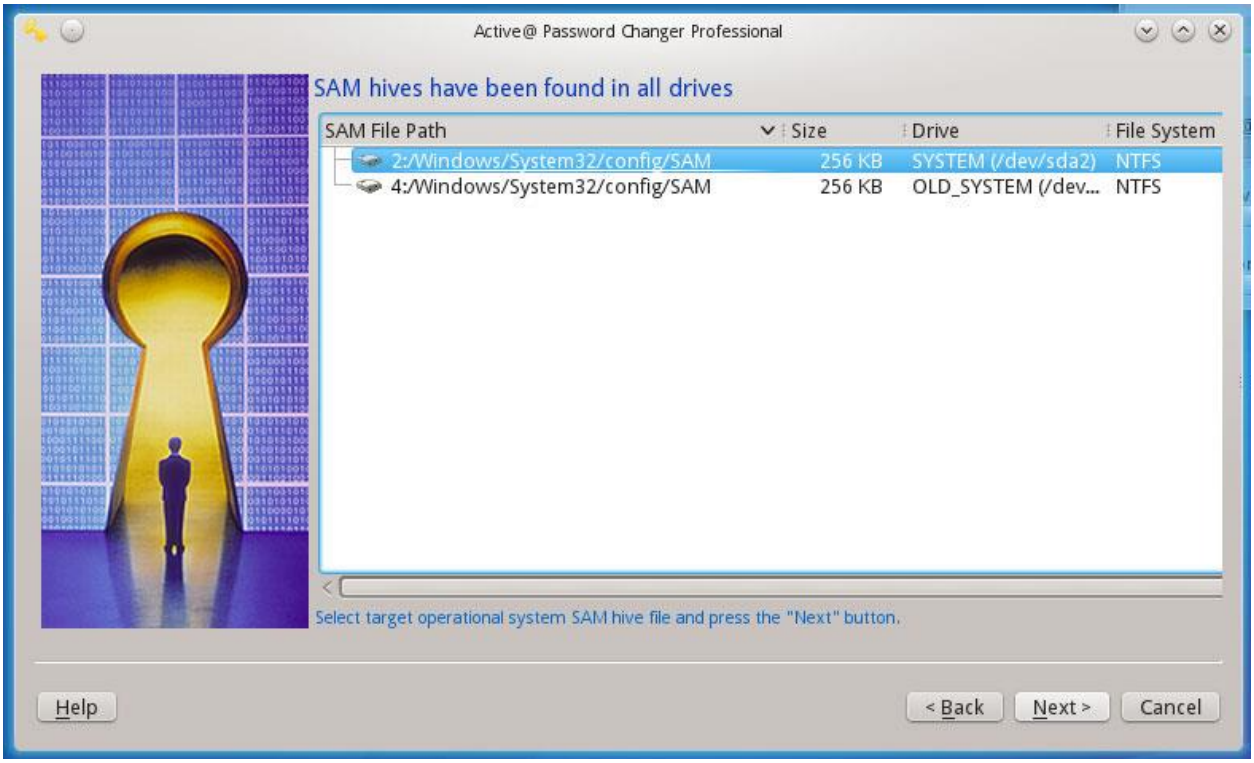
AES encryption

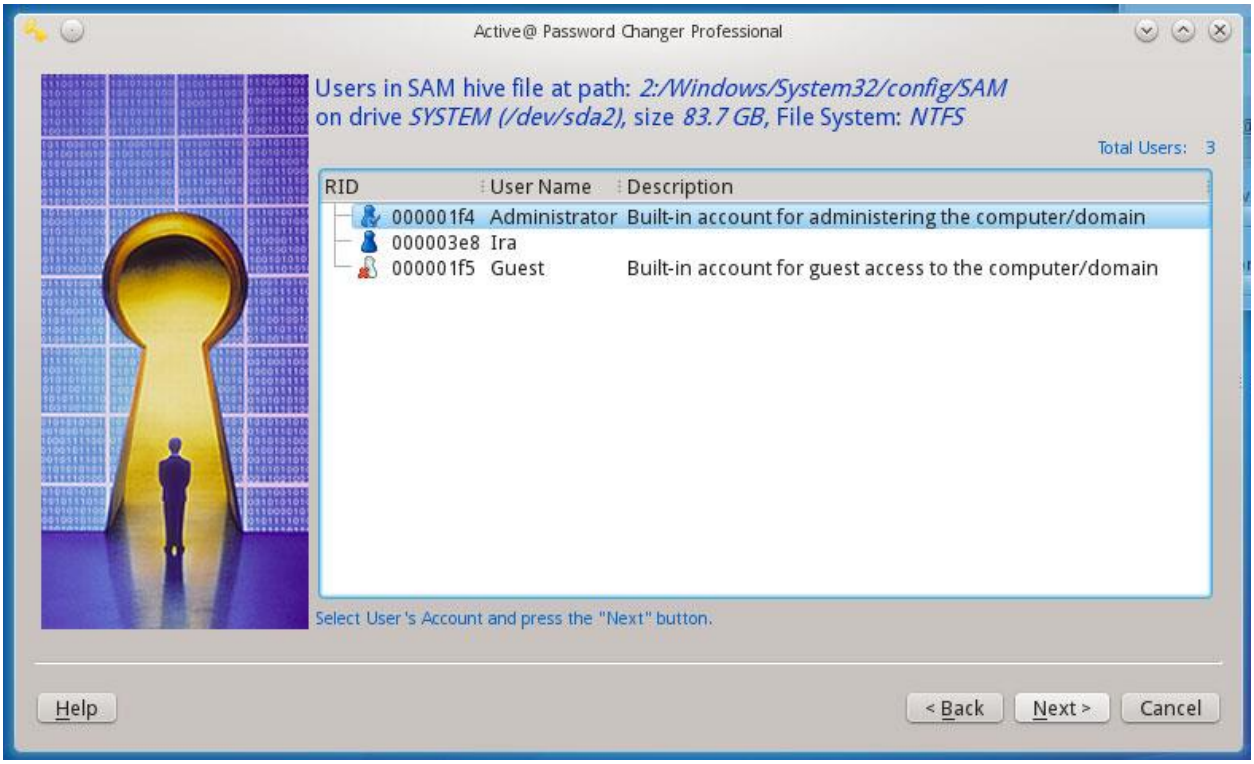


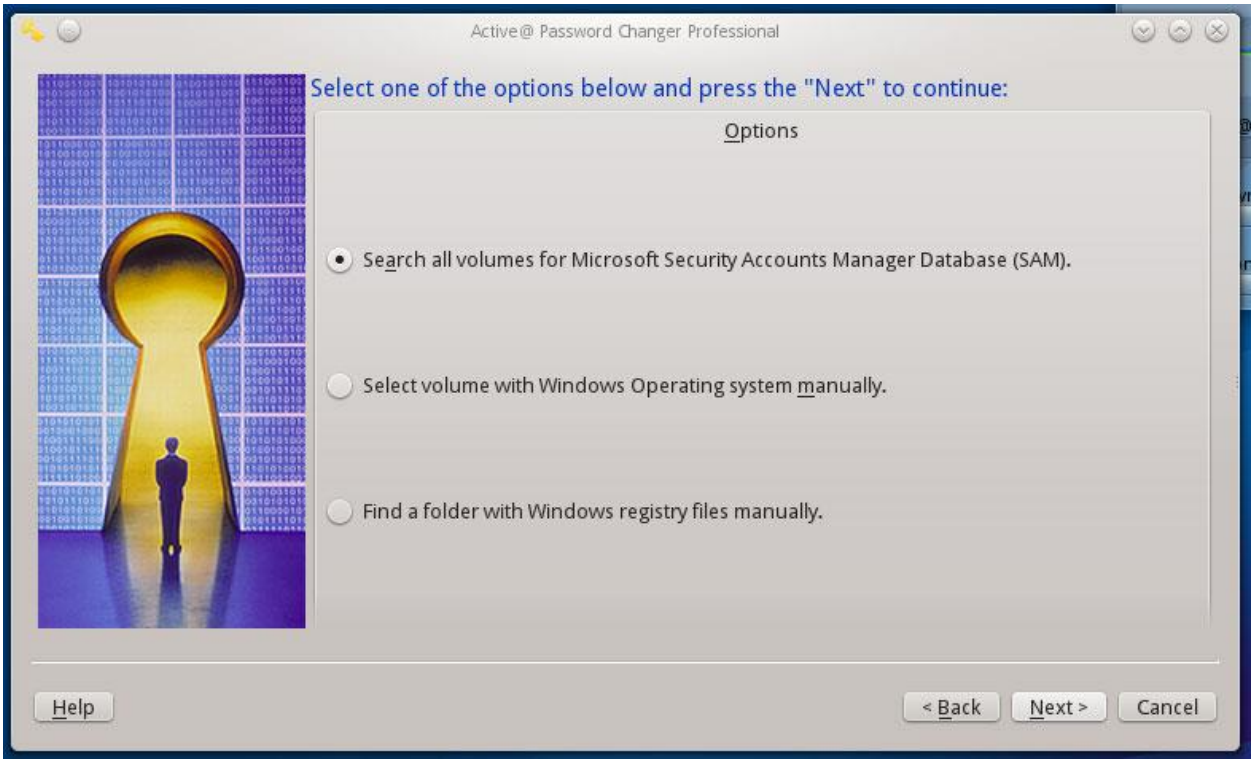
LiveCD

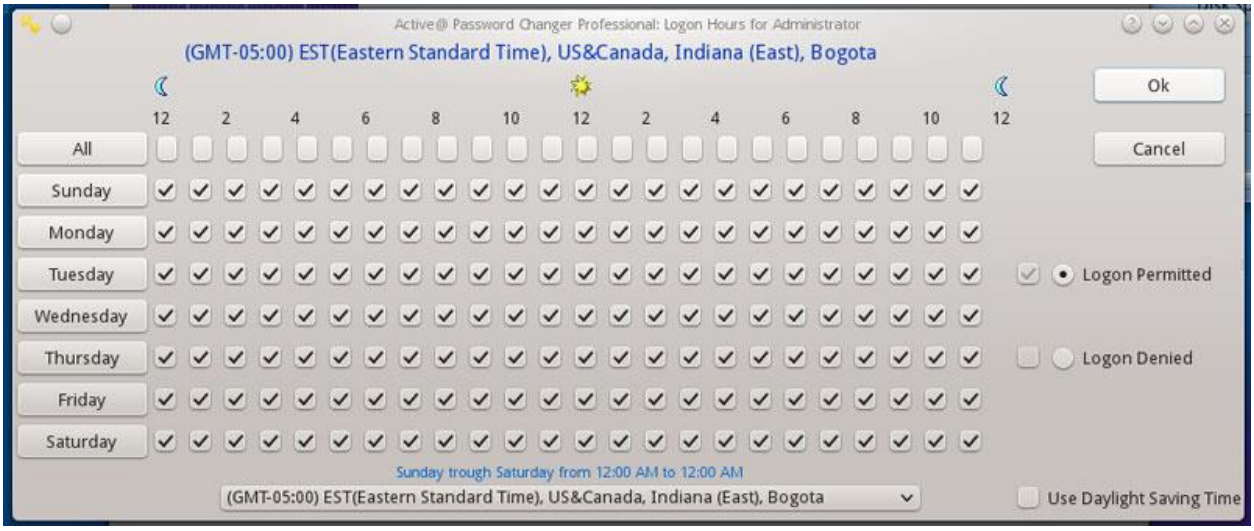


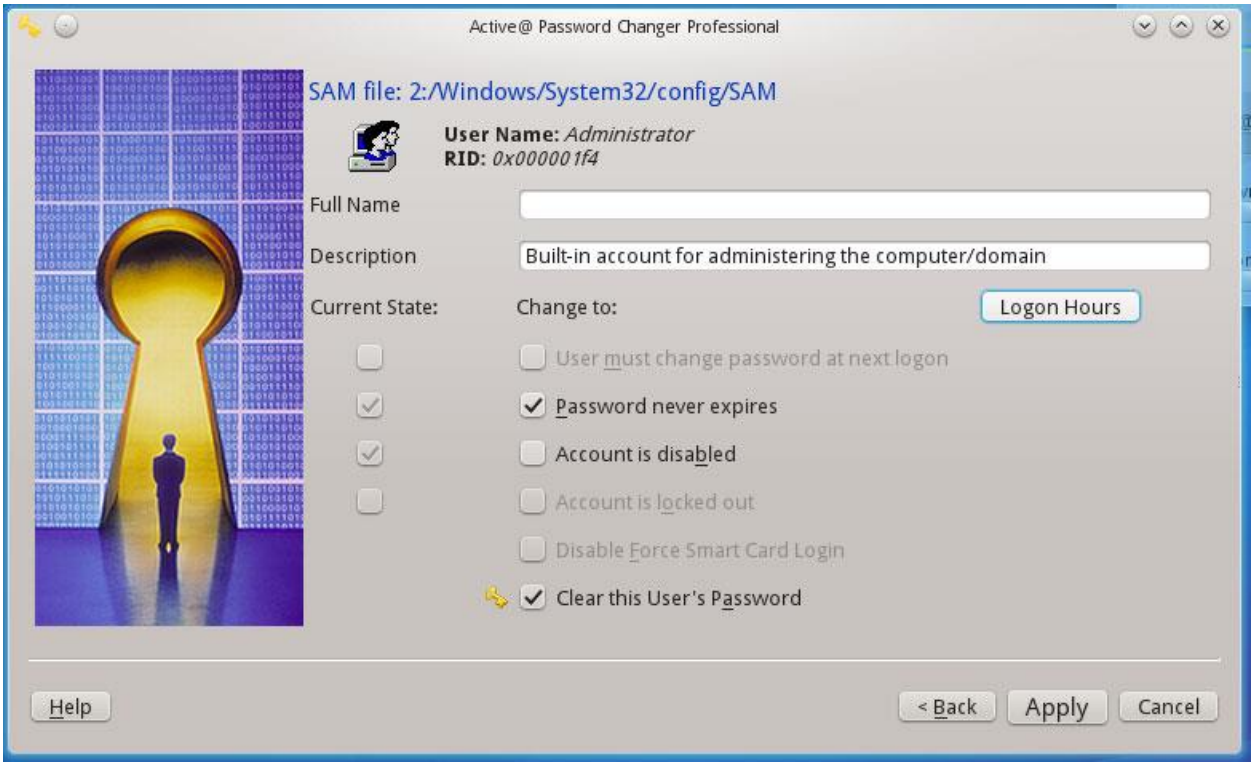

Active@ Password Changer Professional
Active@ Password Changer Professional v.6.0 (build 620)
Active@ Password Changer Professional is a solution designed for resetting local password and account attributes on Windows NT / 2000 / XP / Vista / 2003 / 2008 / Windows7 and Windows8 systems in case the Administrators password is forgotten, lost, or a user account has been blocked, disabled or locked out. You do not need to re-install and re-configure the operating system in this case.
Active@ Password Changer default settings are suitable in most cases.
Licensed to: LSoft
Corporate License
1999-2014 (c) Active Data Recovery Software
www.password-changer.com
Help
Next >
Cancel


Active@ Password Changer Professional
SAM hives have been found in all drives
SAM File Path
Size
Drive
File System
2:/Windows/System32/config/SAM
256 KB
SYSTEM (/dev/sda2)
NTFS
4:/Windows/System32/config/SAM
256 KB
OLD_SYSTEM (/dev...
NTFS
Select target operational system SAM hive file and press the "Next" button.
Help
< Back
Next >
Cancel


Active@ Password Changer Professional
Users in SAM hive file at path: 2:/Windows/System32/config/SAM
on drive SYSTEM (/dev/sda2), size 83.7 GB, File System: NTFS
Total Users: 3
RID
User Name
Description
000001f4 Administrator Built-in account for administering the computer/domain
000003e8 Ira
000001f5 Guest Built-in account for guest access to the computer/domain
Select User's Account and press the "Next" button.
Help
< Back
Next >
Cancel


Active@ Password Changer Professional
Select one of the options below and press the "Next" to continue:
Options
Search all volumes for Microsoft Security Accounts Manager Database (SAM).
Select volume with Windows Operating system manually.
Find a folder with Windows registry files manually.
Help
< Back
Next >
Cancel


Active@ Password Changer Professional: Logon Hours for Administrator
(GMT-05:00) EST(Eastern Standard Time), US&Canada, Indiana (East), Bogota
Ok
Cancel
12 2 4 6 8 10 12 2 4 6 8 10 12
All
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Logon Permitted
Logon Denied
Sunday trough Saturday from 12:00 AM to 12:00 AM
(GMT-05:00) EST(Eastern Standard Time), US&Canada, Indiana (East), Bogota
Use Daylight Saving Time


Active@ Password Changer Professional
SAM file: 2:/Windows/System32/config/SAM
User Name: Administrator
RID: 0x000001f4
Full Name
Description
Built-in account for administering the computer/domain
Current State:
Change to:
Logon Hours
User must change password at next logon
Password never expires
Account is disabled
Account is locked out
Disable Force Smart Card Login
Clear this User's Password
Help
< Back
Apply
Cancel