
ADBLOCK AND WEB SECURITY
BA.NET MANAGED NETWORK
ADMINISTRATOR MANUAL



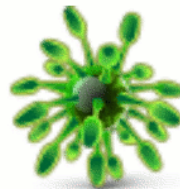
(c) BA.net/Adblock - May 2015



FlashBoot



Server



**Anti-
Malware**



Adblock



AdBlock Filter Server Administrator Manual (c) ba.net adblock@ba.net

Chapter 3, 4 and 5 and portions of other chapters part of Linux HowTo's and Linux Guides copyright Linux Documentation Project LDP.

The optional FlashBoot Software Appliance contains software provided by GNU/Linux, Slackware and other providers covered by the GNU General Public License.

1	Introduction	9
1.1.1	AdBlock BA.net.....	9
1.1.2	Configure AdBlock DNS for iPhone, iPad	9
1.2	<i>Setting up AdBlock BA.net on Android devices</i>	10
1.3	<i>Configure DSL or Wireless router settings.....</i>	10
1.3.1	Configure AdBlock DNS for Mac OS X, Windows, or Linux.....	12
1.4	<i>Works with Safari. Any Web Browser / Any Platform.....</i>	14
1.4.1.1	User Benefits	14
1.4.1.2	Multi Device	14
1.4.1.3	Block Tracking Sites.....	14
1.4.1.4	Block Ads Everywhere.....	14
1.5	<i>Frequently Asked Questions.....</i>	15
1.5.1	Q: How is AdBlock BA.net different from other ad-blocking services ?.....	15
1.5.2	Q: How can it be free ?.....	15
1.5.3	Q: We only use Apple computers in our household, can we still use AdBlock BA.net?.....	15
1.5.4	Q: Will AdBlock BA.net work on my iPhone, Blackberry or other mobile Internet device?	15
1.5.5	Q: Will AdBlock BA.net also restrict pornographic ads?	15
1.5.6	Q: I live in Toronto, will AdBlock BA.net work in Canada?	16
1.5.7	Q: Does AdBlock BA.net track where I go on the Internet?	16
1.5.8	Q: I noticed an ad the other day surfing the web, should I report that to AdBlock BA.net Support?	16
1.5.9	Q: What kind of banners will it block ?	16
1.5.10	What about Site and Blog Owners ?.....	17
1.5.11	Q: Will it block Phishing and Malware sites ?	17
1.5.12	Q: Will it consume Memory like uBlock or AdBlock Plus ?.....	17
1.5.13	Q: Do you have a solution for iPhone on Mobile Networks ?	17
1.5.14	Q: Will VPN affect my mobile battery ?	17
1.5.15	Q: Do you offer Corporate Service ?.....	18
1.5.16	Do you offer Server DNS Filter Solutions ?	18
2	Managed security service.....	20
2.1	<i>Early History of Managed Security Services</i>	<i>21</i>
2.2	<i>Industry terms.....</i>	<i>21</i>
2.3	<i>Six categories of managed security services</i>	<i>21</i>
2.3.1	On-site consulting.....	21

2.3.2	Perimeter management of the client's network	21
2.3.3	Product resale	22
2.3.4	Managed security monitoring	22
2.3.5	Penetration testing and vulnerability assessments	22
2.3.6	Compliance monitoring	22
2.3.7	Engaging an MSSP	23
2.4	<i>Managed security services for mid-sized and smaller businesses</i>	23
3	Filtering methods	25
3.1	<i>Benefits of ad filtering</i>	25
3.2	<i>Economic consequences for online business</i>	27
3.3	<i>Advertiser offensive countermeasures and justifications</i>	27
3.4	<i>Browser integration</i>	28
3.5	<i>External programs</i>	29
3.6	<i>Hosts file</i>	29
3.7	<i>DNS cache</i>	29
3.8	<i>DNS filtering</i>	30
3.9	<i>Ad filtering by external parties and internet providers</i>	30
4	BA.net Adblock Filter Server CLOUD	30
4.1	<i>Children's Internet Protection Act</i>	34
4.1.1.1	Background	34
4.1.1.2	What CIPA Requires	34
5.0	<i>BA.net Adblock Speed VPN for iPhone Config</i>	36
4.1.2	FAQ	42
5	Corporate Proxy auto-config PAC	44
5.1	<i>Context</i>	44
5.2	<i>Proxy configuration</i>	44
5.3	<i>The PAC File</i>	45
5.3.1	Limitations	46
5.3.1.1	PAC Character-Encoding	46
5.3.1.2	DnsResolve	46
5.3.1.3	myIpAddress	47
5.3.1.4	Security	47
5.3.1.5	Others	48
5.3.2	Advanced functionality	48
6	BA.NET Adblock Speed VPN for iPhone	48

6.1	<i>VPN connectivity overview</i>	49
6.2	<i>VPN Type</i>	50
6.3	<i>Security mechanisms</i>	52
6.3.1	<i>Authentication</i>	54
6.4	<i>Routing</i>	54
6.4.1	Provider-provisioned VPN building-blocks	55
6.4.2	<i>OSI Layer 2 services</i>	56
6.4.3	<i>OSI Layer 3 PPVPN architectures</i>	58
6.4.4	<i>Unencrypted tunnels</i>	59
6.5	<i>Trusted delivery networks</i>	60
6.6	<i>VPNs in mobile environments</i>	61
6.7	<i>VPN on Routers</i>	62
6.8	<i>Networking limitations</i>	63
7	How DNS Works	64
7.1	<i>Name Lookups with DNS</i>	68
7.2	<i>Types of Name Servers</i>	69
7.3	<i>The DNS Database</i>	70
7.4	<i>Reverse Lookups</i>	72
7.4.1	<i>Notes</i>	73
8	Running named	74
8.1	<i>The named.boot File</i>	74
8.2	<i>The BIND 8 host.conf File</i>	77
8.3	<i>The DNS Database Files</i>	79
8.4	<i>Caching-only named Configuration</i>	84
8.5	<i>Writing the Master Files</i>	85
8.6	<i>Verifying the Name Server Setup</i>	87
8.7	<i>Other Useful Tools</i>	90
8.7.1	<i>Notes</i>	90
9	BA.net Adblock Filter Server FlashBoot	91
9.1.1	HOWTO INSTALL	92
10	Configuration Files	94
10.1	<i>2 Initial configuration</i>	94
10.2	<i>3 Internals and externals</i>	96

10.3	4 Security.....	99
10.4	5 Configuration files.....	99
10.4.1	5.1 /etc/bind/named.conf.local.....	99
10.4.2	5.2 /etc/bind/externals/db.example.com.....	100
10.4.3	5.3 /etc/bind/internals/db.example.com.....	101
10.4.4	Bibliography.....	101
10.4.5	Footnotes.....	101
11	Domain Name Server (DNS) Configuration and Administration.....	102
12	Response Rate Limiting.....	106
12.1	The Problem.....	106
12.2	A Solution.....	107
12.3	The Results.....	107
12.4	Sample BIND RRL configuration.....	107
13	OpenVPN.....	109
13.1	Determining whether to use a routed or bridged VPN.....	109
13.2	Numbering private subnets.....	109
13.3	Setting up your own Certificate Authority (CA) and generating certificates and keys for an OpenVPN server and multiple clients.....	110
13.3.1	Overview.....	110
13.3.2	Generate the master Certificate Authority (CA) certificate & key.....	112
13.3.3	Generate certificate & key for server.....	113
13.3.4	Generate certificates & keys for 3 clients.....	114
13.3.5	Generate Diffie Hellman parameters.....	114
13.3.6	Key Files.....	116
13.4	Creating configuration files for server and clients.....	117
13.4.1	Getting the sample config files.....	117
13.4.2	Editing the server configuration file.....	117
13.4.3	Editing the client configuration files.....	119
13.5	Starting up the VPN and testing for initial connectivity.....	119
13.5.1	Starting the server.....	119
13.5.2	Starting the client.....	121
13.5.3	Troubleshooting.....	121
13.6	Configuring OpenVPN to run automatically on system startup.....	123
13.6.1	Linux.....	123
13.6.2	Windows.....	123
13.7	Controlling a running OpenVPN process.....	124
13.7.1	Running on Linux/BSD/Unix.....	124
13.7.2	Running on Windows as a GUI.....	124

13.7.3	Running in a Windows command prompt window	124
13.7.4	Running as a Windows Service	125
13.7.5	Modifying a live server configuration	125
13.7.6	Status File.....	125
13.7.7	Using the management interface.....	126
13.8	<i>Expanding the scope of the VPN to include additional machines on either the client or server subnet.</i>	127
13.8.1	Including multiple machines on the server side when using a routed VPN (dev tun)	128
13.8.2	Including multiple machines on the server side when using a bridged VPN (dev tap)	128
13.8.3	Including multiple machines on the client side when using a routed VPN (dev tun)	128
13.8.4	Including multiple machines on the client side when using a bridged VPN (dev tap)	130
13.9	<i>Pushing DHCP options to clients</i>	131
13.10	<i>Configuring client-specific rules and access policies</i>	131
13.10.1	ccd/sysadmin1	133
13.10.2	ccd/contractor1	133
13.10.3	ccd/contractor2.....	133
13.11	<i>Using alternative authentication methods</i>	134
13.11.1	Using Script Plugins	135
13.11.2	Using Shared Object or DLL Plugins	135
13.11.3	Using username/password authentication as the only form of client authentication	136
13.12	<i>How to add dual-factor authentication to an OpenVPN configuration using client-side smart cards</i>	137
13.12.1	About dual-factor authentication	137
13.12.2	What is PKCS#11?	138
13.12.3	Finding PKCS#11 provider library	139
13.12.4	How to configure cryptographic token	139
13.12.5	How to modify an OpenVPN configuration to make use of cryptographic tokens	140
13.12.5.1	Determine the correct object.....	140
13.12.5.2	Using OpenVPN with PKCS#11	140
13.12.5.2.1	A typical set of OpenVPN options for PKCS#11	141
13.12.5.2.2	Advanced OpenVPN options for PKCS#11.....	141
13.12.5.3	PKCS#11 implementation considerations	141
13.12.5.4	OpenSC PKCS#11 provider	141
13.12.6	Difference between PKCS#11 and Microsoft Cryptographic API (CryptoAPI)	142
13.13	<i>Routing all client traffic (including web-traffic) through the VPN</i>	142
13.13.1	Overview	142

13.13.2	Implementation	143
13.13.3	Caveats	144
13.14	<i>Running an OpenVPN server on a dynamic IP address</i>	144
13.15	<i>Connecting to an OpenVPN server via an HTTP proxy.</i>	145
13.16	<i>Connecting to a Samba share over OpenVPN</i>	146
13.17	<i>Implementing a load-balancing/failover configuration</i>	147
13.17.1	Client	147
13.17.2	Server	149
13.18	<i>Hardening OpenVPN Security</i>	149
13.18.1	tls-auth	149
13.18.2	proto udp	150
13.18.3	user/group (non-Windows only)	150
13.18.4	Unprivileged mode (Linux only)	150
13.18.5	chroot (non-Windows only)	152
13.18.6	Larger RSA keys	152
13.18.7	Larger symmetric keys	152
13.18.8	Keep the root key (ca.key) on a standalone machine without a network connection	153
13.19	<i>Revoking Certificates</i>	153
13.19.1	Example	153
13.19.2	CRL Notes	154
13.20	<i>Important Note on possible "Man-in-the-Middle" attack if clients do not verify the certificate of the server they are connecting to.</i>	155
13.21	<i>Sample OpenVPN 2.0 configuration files</i>	157
13.21.1	sample-config-files/server.conf	158
13.21.2	sample-config-files/client.conf	165

1 INTRODUCTION

1.1.1 ADBLOCK BA.NET

Make your Internet **Faster**, more Private and Safer with AdBlock BA.net.



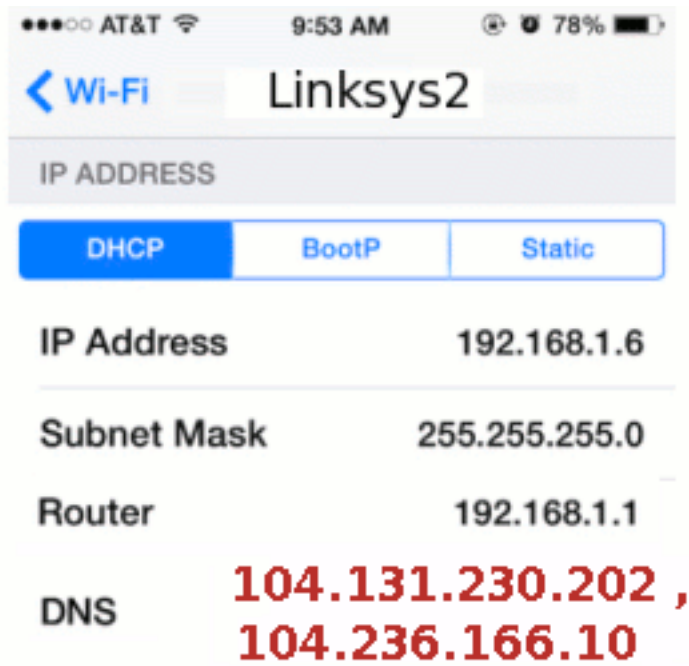
Works on iPad, IOS, Mac, PC. No software to install. It is a network based DNS Service.

Provide Network Security and Control without dedicated staff

[104.131.230.202](#) , 104.236.166.10 (demo servers)

1.1.2 CONFIGURE ADBLOCK DNS FOR IPHONE, IPAD

- Open Settings
- Tap on "WiFi" and tap the blue arrow alongside the wi-fi network name you are connected to
- Tap the numbers next to "DNS" to change them



Free BA.net AdBlock DNS

104.131.230.202 , 104.236.166.10



1.2 SETTING UP ADBLOCK BA.NET ON ANDROID DEVICES

1. Settings
2. WiFi (click on word "WiFi", not ON/OFF switch)
3. Press and hold preferred (or active) wireless network until dialog pops up
4. Select "Modify Network"
5. Check "Show advanced options" checkbox at the bottom
6. Switch "IP settings" to "Static"
7. Keep IP address, Gateway and Network prefix length the same (should be set from standard DHCP)
8. Set DNS 1 and DNS 2 fields as per table below:
9. "Save"
10. Restart your phone (power cycle).

1.3 CONFIGURE DSL OR WIRELESS ROUTER SETTINGS

Depending on your router manufacturer, the steps to configure the router may vary. Following steps are provided for your reference. For more information, you may refer to the support documentation for the router.



1. Start your Web browser.
2. In the Address box, type the IP address of your router, and then press Enter.

Generally, 192.168.1.1 and 192.168.0.1 are the most widely used default IP addresses by various manufacturers. If your router manufacturer uses a different IP address, refer to the help documentation for the router.

3. Type the administrator user name and password, and then click OK.

Router configuration settings page opens in your Web browser.

4. Find and open the DNS settings.

You may find the DNS settings option under WAN settings.

5. In the Preferred DNS server and Alternate DNS server boxes, type the DNS server addresses provided by your Internet service provider.

Use the following server BA.net AdBlock DNS addresses:

104.131.230.202 , 104.236.166.

6. Click Apply or Save or Save Settings.
7. Restart your router to apply the changes.

1.3.1 CONFIGURE ADBLOCK DNS FOR MAC OS X, WINDOWS, OR LINUX

- [Mac OS X](#)
- [Windows](#)
- [Linux](#)
- [DSL or Wireless Router](#)
- [Android](#)
- [AdBlock Server](#)

After BA.net/adblock



Before BA.net/adblock



1.4 WORKS WITH SAFARI. ANY WEB BROWSER / ANY PLATFORM

1.4.1.1 User Benefits

The benefits of ad blocking include quicker loading and cleaner looking Web pages free from advertisements, lower resource waste (bandwidth, CPU, memory, etc.), and privacy benefits gained through the exclusion of the tracking and profiling systems of ad delivery platforms.

1.4.1.2 Multi Device

You can configure it for your computers, iPad, iPhone WiFi and more devices on your network. [Premium Plans](#) available.

Except on iPhone mobile networks, as DNS can not be changed. It will work on WiFi for iPhone.

1.4.1.3 Block Tracking Sites

Many sites use Web bugs and analytics to track where you go on the Internet. AdBlock BA.net stops these sites from profiling you, invading your privacy and slowing your connection.

1.4.1.4 Block Ads Everywhere

AdBlock BA.net stops advertisements on Safari, Any Web Browser, Any Platform. Also blocks many in-app Ads! Also blocks Ads from appearing in MSN, Yahoo!, and AOL messaging programs at the source. No more annoying pop-up animated ads.

1.5 FREQUENTLY ASKED QUESTIONS

1.5.1 Q: HOW IS ADBLOCK BA.NET DIFFERENT FROM OTHER AD-BLOCKING SERVICES ?

AdBlock BA.net does not require installing any software on your computer and works with any Web browser on any computer.

1.5.2 Q: HOW CAN IT BE FREE ?

AdBlock BA.net is free for personal use. If you like the service we encourage you to [Share it with your friends](#). Or upgrade to a [Premium Plan](#)

1.5.3 Q: WE ONLY USE APPLE COMPUTERS IN OUR HOUSEHOLD, CAN WE STILL USE ADBLOCK BA.NET?

Yes, AdBlock BA.net will work with Safari, Firefox, etc. on Apple computers.

1.5.4 Q: WILL ADBLOCK BA.NET WORK ON MY IPHONE, BLACKBERRY OR OTHER MOBILE INTERNET DEVICE?

Yes, although some providers give no option to configure your DNS servers in order to use AdBlock BA.net. (For example it will not work on 3G connections only on WiFi)

1.5.5 Q: WILL ADBLOCK BA.NET ALSO RESTRICT PORNOGRAPHIC ADS?

AdBlock BA.net is not specifically designed to remove pornographic ads, however we make every attempt to block ads from known ad distribution networks.

1.5.6 Q: I LIVE IN TORONTO, WILL ADBLOCK BA.NET WORK IN CANADA?

Yes, Adblock BA.net will work from any location, however we concentrate our efforts on blocking advertising on the most popular sites for U.S. Internet users.

You can report any Ads or Malware to be included in the BA.net/adblock blocked list. [Report Ads or Malware Here](#). So far our blocked list contains over 180.000 domains!

1.5.7 Q: DOES ADBLOCK BA.NET TRACK WHERE I GO ON THE INTERNET?

Adblock BA.net does not log any personally identifiable information. See details at the [Privacy Policy](#)

1.5.8 Q: I NOTICED AN AD THE OTHER DAY SURFING THE WEB, SHOULD I REPORT THAT TO ADBLOCK BA.NET SUPPORT?

Adblock BA.net will not block 100% of Internet advertising. Our goal is to eliminate banner and Flash advertisements on the most popular sites, and block the most widely used advertising distributors.

You can report any Ads or Malware to be included in the BA.net/adblock blocked list. [Report Ads or Malware Here](#). So far our blocked list contains over 180.000 domains!

1.5.9 Q: WHAT KIND OF BANNERS WILL IT BLOCK ?

Adblock BA.net is designed to block Banner and Flash advertising on the most popular sites, and to block ads coming from the largest advertising networks.

Adblock BA.net will work for anyone, anywhere in the world, but our focus is on popular U.S. Websites. Our servers are located in the US East Coast, US West Coast and EU London.

1.5.10 WHAT ABOUT SITE AND BLOG OWNERS ?

Our intent is to block major adserver networks that track you across the web. They use questionable re-targetting, profiling and invade your privacy.

Smaller sites generally offer sponsorships and directly served ads, which we do not block.

1.5.11 Q: WILL IT BLOCK PHISHING AND MALWARE SITES ?

Yes Phishing and Malware sites will also be blocked. Helping to keep you safe from identity theft. So far our blocked list contains over 180.000 domains!

1.5.12 Q: WILL IT CONSUME MEMORY LIKE UBLOCK OR ADBLOCK PLUS ?

uBlock or other Browser add-ons can consume a lot of memory on your computer. As they have to process over 100k rules and domains to block. Our DNS solution moves that processing to our servers, we block 180k adware and malware domains! You will need less memory and have a faster and safer internet. No need to install any add-on or plug-in, just configure our DNS and you are ready to go.

1.5.13 Q: DO YOU HAVE A SOLUTION FOR IPHONE ON MOBILE NETWORKS ?

Yes, AdBlock Speed VPN for iPhone. Contact us at adblock@ba.net to get a Business Dedicated Adblock VPN Server.

1.5.14 Q: WILL VPN AFFECT MY MOBILE BATTERY ?

Short answer no. A PPTP VPN plus BA.net Adblock DNS is the ideal way to surf faster on iPhone on mobile networks. AdBlock will speed up your connection and PPTP is the vpn protocol that will impact your battery usage the least.

PPTP is not 100% safe as an encryption protocol, but it provides adequate protection for guest hotspot surfing, and adblock usage. The best feature of PPTP is that it is native to the iphone, it is simple to

configure and will add the least amount of overhead to your battery usage.

The Adblock data transmission and CPU savings will combine with the low overhead of PPTP to a negligible impact on your iPhone battery.

1.5.15 Q: DO YOU OFFER CORPORATE SERVICE ?

Yes, you can point your corporate routers to our Filtering DNS service. We offer volume discounts per user.

Also available custom filter lists and access policies running on your own dedicated virtual dns servers.

Corporate, ISP, school and campus filtering bundles also available.

- [Get Premium Adblock Multi Device](#)
- [Business Web Security Solutions](#)

[Wikipedia Ad Filtering Docs](#)

[Wikipedia VPN Docs](#)

1.5.16 DO YOU OFFER SERVER DNS FILTER SOLUTIONS ?

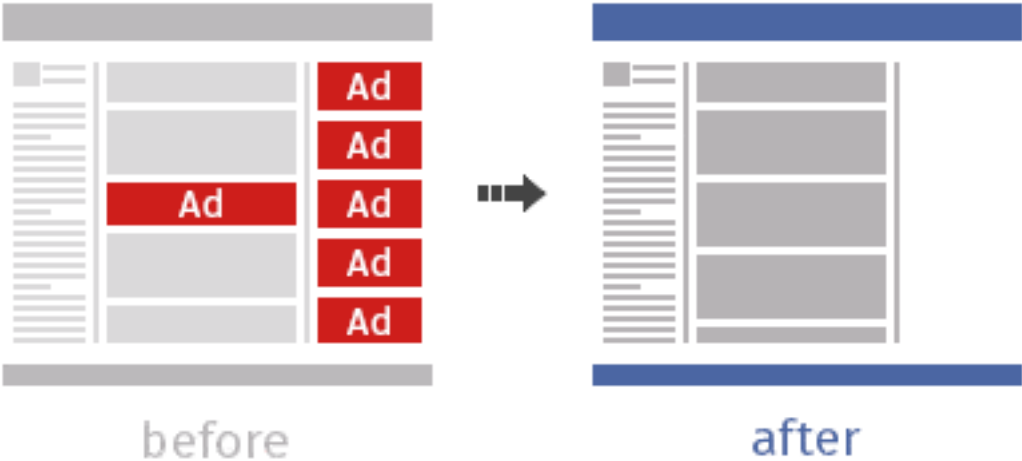
BA.net Adblock DNS Server Managed is a complete Software Appliance. Built in a simple USB Flash Boot package. [Free Download](#)

- Q: Do you offer an Administrator Manual ?

You can download a free preview of the Administrator Manual [here](#)



[950k pdf](#)



2 MANAGED SECURITY SERVICE

In [computing](#), managed security services (MSS) are [network security](#) services that have been [outsourced](#) to a [service provider](#). A company providing such a service is a managed security service provider (MSSP)^[1] The roots of MSSPs are in the [Internet Service Providers](#) (ISPs) in the mid to late 1990's. Initially ISPs would sell customers a [firewall](#) appliance, as [customer premises equipment](#) (CPE), and for an additional fee would manage the customer-owned firewall over a dial-up connection.^[2]

According to recent industry research, most organizations (74%) manage IT security in-house, but 82% of IT professionals said they have either already partnered with, or plan to partner with, a managed security service provider.^[3]

Businesses turn to managed security services providers to alleviate the pressures they face daily related to information security such as targeted malware, customer data theft, skills shortages and resource constraints.^[4]

Managed security services (MSS) are also considered the systematic approach to managing an organization's security needs. The services may be conducted in-house or outsourced to a service provider that oversees other companies' network and information system security. Functions of a managed security service include round-the-clock monitoring and management of intrusion detection systems and firewalls, overseeing patch management and upgrades, performing security assessments and security audits, and responding to emergencies. There are products available from a number of vendors to help organize and guide the procedures involved. This diverts the burden of performing the chores manually, which can be considerable, away from administrators.

Industry research firm Forrester Research in late 2014 identified the 13 most significant vendors in the North American market with its 26-criteria evaluation of managed security service providers (MSSPs)--identifying [IBM](#), Dell [SecureWorks](#), [Trustwave](#), [AT&T](#), [Verizon](#) and others as the leaders in the MSSP market.^[5]

2.1 EARLY HISTORY OF MANAGED SECURITY SERVICES

An earliest example of a cloud-based MSSP service is [US West](#) INTERACT Internet Security. The security service didn't require the customer to purchase any equipment and no security equipment was installed at the customers premises.^[6] The service is considered a MSSP offering in that US West retained ownership of the firewall equipment and the firewalls were operated from their own Internet [Point of Presence](#) (PoP)^[7] The service was based on [Check Point](#) Firewall-1 equipment.^[8] Following over a year long beta introduction period, the service was generally available by early 1997.^{[6][7]} The service also offered managed Virtual Private Networking (VPN) encryption security at launch.^[7]

2.2 INDUSTRY TERMS

- Asset: A resource valuable to a company worthy of protection.
- Incident: An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an asset.
- Alert: Identified information, i.e. fact, used to correlate an incident.

2.3 SIX CATEGORIES OF MANAGED SECURITY SERVICES

2.3.1 ON-SITE CONSULTING

This is customized assistance in the assessment of business risks, key business requirements for security and the development of security policies and processes. It may include comprehensive security architecture assessments and design (include technology, business risks, technical risks and procedures). Consulting may also include security product integration and On-site mitigation support after an intrusion has occurred, including emergency incident response and forensic analysis^{[1][9]}

2.3.2 PERIMETER MANAGEMENT OF THE CLIENT'S NETWORK

This service involves installing, upgrading, and managing the [firewall](#), [Virtual Private Network](#) (VPN) and/or intrusion detection hardware and software, [electronic mail](#), and commonly performing configuration

changes on behalf of the customer. Management includes monitoring, maintaining the firewall's traffic routing rules, and generating regular traffic and management reports to the customer.^[1] [Intrusion detection](#) management, either at the network level or at the individual host level, involves providing intrusion alerts to a customer, keeping up to date with new defenses against intrusion, and regularly reporting on intrusion attempts and activity. Content filtering services may be provided by; such as, [email filtering](#)) and other data traffic filtering.^[9]

2.3.3 PRODUCT RESALE

Clearly not a managed service by itself, product resale is a major revenue generator for many MSS providers. This category provides value-added hardware and software for a variety of security-related tasks. One such service that may be provided is archival of customer data.^[9]

2.3.4 MANAGED SECURITY MONITORING

This is the day-to-day monitoring and interpretation of important system events throughout the network—including unauthorized behavior, malicious hacks, [denial of service](#) (DoS), anomalies, and trend analysis. It is the first step in an incident response process.

2.3.5 PENETRATION TESTING AND VULNERABILITY ASSESSMENTS

This includes one-time or periodic software scans or hacking attempts in order to find vulnerabilities in a technical and logical perimeter. It generally does not assess security throughout the network, nor does it accurately reflect personnel-related exposures due to disgruntled employees, social engineering, etc. Regularly, reports are given to the client.^{[1][9]}

2.3.6 COMPLIANCE MONITORING

This includes monitoring event logs not for intrusions, but change management. This service will identify changes to a system that violate a formal security policy for example, if a rogue administrator grants

himself or herself too much access to a system. In short, it measures compliance to a technical risk model.

2.3.7 ENGAGING AN MSSP

The decision criteria for engaging the services of an MSSP are much the same as those for any other form of outsourcing: cost-effectiveness compared to in-house solutions, focus upon core competencies, need for round-the-clock service, and ease of remaining up-to-date. An important factor, specific to MSS, is that outsourcing network security hands over critical control of the company's infrastructure to an outside party, the MSSP, whilst not relieving the ultimate responsibility for errors. The client of an MSSP still has the ultimate responsibility for its own security, and as such must be prepared to manage and monitor the MSSP, and hold it accountable for the services for which it is contracted. The relationship between MSSP and client is not a turnkey one.^[1]

Although the organization remains responsible for defending its network against information security and related business risks, working with an MSSP allows the organization to focus on its core activities while remaining protected against network vulnerabilities.

Business risks can result when information assets upon which the business depends are not securely configured and managed (resulting in asset compromise due to violations of confidentiality, availability, and integrity). Compliance with specific government-defined security requirements can be achieved by using managed security services.^[10]

2.4 MANAGED SECURITY SERVICES FOR MID-SIZED AND SMALLER BUSINESSES

The business model behind managed security services is commonplace among large enterprise companies with their IT security experts. The model was later adapted to fit medium-sized and smaller companies (SMBs - organizations up to 500 employees, or with no more than 100 employee at any one site) by the value-added reseller (VAR) community, either specializing in managed security or offering it as an extension to their managed IT service solutions. SMBs are increasingly turning to managed security services for a number of

reasons. Chief among these are the specialized, complex and highly dynamic nature of IT security and the growing number of regulatory requirements obliging businesses to secure the digital safety and integrity of personal information and financial data held or transferred via their computer networks.

Whereas larger organizations typically employ an IT specialist or department, organizations at a smaller scale such as distributed location businesses, medical or dental offices, attorneys, professional services providers or retailers do not typically employ full-time security specialists, although they frequently employ IT staff or external IT consultants. Of these organizations, many are constrained by budget limitations. To address the combined issues of lack of expertise, lack of time and limited financial resources, an emerging category of managed security service provider for the SMB has arisen.

Services providers in this category tend to offer comprehensive IT security services delivered on remotely managed appliances or devices that are simple to install and run for the most part in the background. Fees are normally highly affordable to reflect financial constraints, and are charged on a monthly basis at a flat rate to ensure predictability of costs. Service providers deliver daily, weekly, monthly or exception-based reporting depending on the client's requirements.^[11]

3 FILTERING METHODS

An extremely common method of filtering is simply to block (or prevent autoplay of) Flash animation or image loading or Windows audio and video files. This can be done in most browsers easily. This crude technological method is refined by numerous [browser extensions](#). Every internet browser handles this task differently, but, in general, one alters the options, preferences or application extensions to filter specific media types. An additional add-on is usually required to differentiate between ads and non-ads using the same technology, or between wanted and unwanted ads or behaviors.

The more advanced filters allow fine-grained control of [advertisements](#) through features such as [blacklists](#), [whitelists](#), and [regular expression](#) filters. Certain security features also have the effect of disabling some ads. Some [antivirus](#) software can act as an ad blocker.

Filtering by intermediaries such as providers or national governments is increasingly common. See below especially re provider ad substitution and national root DNS.

3.1 BENEFITS OF AD FILTERING

To users, the benefits of ad blocking include quicker loading and cleaner looking Web pages free from advertisements, lower resource waste (bandwidth, CPU, memory, etc.), and privacy benefits gained through the exclusion of the tracking and profiling systems of ad delivery platforms. Blocking ads can also save minimal amounts of energy.^[2]

Users who pay for total transferred bandwidth ("capped" or pay-for-usage connections) including most mobile users worldwide, have a direct financial benefit from filtering an ad before it is loaded. Streaming audio and video, even if they are not presented to the user interface, can rapidly consume gigabytes of transfer especially on a faster 4G connection. In Canada, where users without a data plan often pay C\$0.50/megabyte (\$500/gigabyte) for at least the first 50-100MB exceeding their data allowance, the cost of tolerating ads can be intolerable. Even fixed connections are often subject to usage limits, especially the faster connections (100Mbit/s and up) which can quickly saturate a network if filled by streaming media. "The extent of unlimited bandwidth plans is often grossly over-estimated by US and European users and advertisers. This problem affects other countries, especially those with bandwidth limitations on their global Internet connections, or those that have poor regulatory or effective monopoly providers."

To advertisers, the benefits include not angering or annoying users into blocking, defaming or boycotting their products or websites. Few advertisers actually intend to anger end users. Very sophisticated filtering and [anti-spam](#) techniques can involve active defenses which can shut down an advertiser's domains or brokers, ban them from searches or target them for other countermeasures. Some countries have even considered banning the use of certain ports, e.g. South Korea's proposed ban on port 25 used by [SMTP](#).^[3] Future countermeasures would be likely to include bans on ads South Koreans are unlikely to want or even ad brokering services. Ad substituting is also a legal and common practice already, for instance in Canadian cable TV where regulations permit showing a Canadian channel with Canadian ads instead of a US channel with US ads, where both are broadcasting the show simultaneously - this practice has spread to the web with some cable Internet providers uniformly substituting foreign ads for local ones, for which they receive a share of the revenue. Avoiding national, provider or technological interference with their ads is a priority for advertisers and especially brokers of advertising, to whom it could be fatal.

3.2 ECONOMIC CONSEQUENCES FOR ONLINE BUSINESS

One consequence of widespread ad blocking is decreased revenue to a website sustained by advertisements,^[4] where this blocking can be detected.

A number of website operators, who use online advertisements to fund the hosting of their websites, argue that the use of ad-blocking software risks cutting off their revenue stream. While some websites have successfully implemented subscription and membership based systems for revenue, the majority of websites today rely on online advertising to function.

3.3 ADVERTISER OFFENSIVE COUNTERMEASURES AND JUSTIFICATIONS

Some websites have taken counter-measures against ad-blocking software, such as attempting to detect the presence of ad blockers and informing users of their views, or outright preventing users from accessing the content unless they disable the ad-blocking software. There have been several arguments supporting^[5] and opposing^[6] the assertion that blocking ads is wrong.^[7]

3.4 BROWSER INTEGRATION



[Wikitravel](#) with and without [Adblock Plus](#)

Almost all modern [web browsers](#) block unsolicited [pop-up ads](#) by default. [Opera](#), [Konqueror](#), [Maxthon 2](#), and [Internet Explorer 8](#)^[8] also include content filtering, which prevents external files such as images or JavaScript files from loading. Content filtering can be added to [Mozilla Firefox](#) and related browsers with [Adblock Plus](#), and a number of sources provide regularly updated filter lists. For [Internet Explorer](#) there are several add-ons available like [Simple Adblock](#), and [Quero](#) that also allows users to temporarily unblock blocked content. A rudimentary content blocking feature is integrated in [Opera](#) and does not require an add-on. For Google Chrome, which has had extensions available since v2.0, extensions are available, such as [Adblock](#), [AdSweep](#), [FlashBlock](#), [Adblock Plus](#) and [AdblockforChrome](#). Another method for filtering advertisements uses [CSS](#) rules to hide specific [HTML](#) and [XHTML elements](#).

3.5 EXTERNAL PROGRAMS

A number of external applications offer ad filtering as a primary or additional feature. A traditional solution is to customize an [HTTP proxy](#) (or web proxy) to filter content. These programs work by caching and filtering content before it is displayed in a user's browser. This provides an opportunity to remove not only ads but also content which may be offensive, inappropriate, or simply junk. Popular proxy software which blocks content effectively include [AdGuard](#), [Privoxy](#), [Squid](#), [Ad Muncher](#) and [Diladele Web Safety](#). The main advantage of the method is freedom from implementation limitations (browser, working techniques) and centralization of control (the proxy can be used by many users). The major drawback is that the proxy sees only raw content and thus it's difficult to handle [JavaScript](#)-generated content.

3.6 HOSTS FILE

Further information: [hosts file](#).

This method exploits the fact that most operating systems store a file with IP address, domain name pairs which is consulted by most browsers before using a DNS server to look up a domain name. By assigning the [loopback address](#) to each known [ad server](#), the user directs traffic intended to reach each [ad server](#) to the local machine. Running a suitable web server locally the ad content can be replaced with anything the user wishes.

3.7 DNS CACHE

This method operates by filtering and changing records of a DNS cache. On most operating systems the domain name resolution always goes via DNS cache. By changing records within the cache or preventing records from entering the cache, programs are allowed or prevented from accessing domain names. The external programs like [Portable DNS Cache and Firewall](#) ^[9] monitor internal DNS cache and import DNS records from a file. As a part of the domain name resolution process, a DNS cache lookup is performed before contacting a DNS server. Thus its records take precedence over DNS server queries. Unlike the method of modifying a Hosts file, this

method is more flexible as it uses more comprehensive data available from DNS cache records.

3.8 DNS FILTERING

Advertising can be blocked by using a DNS server which is configured to block access to domains or hostnames which are known to serve ads.^[10]

Morally, while some argue that domain name holders are owners of property (and have been found to have such rights in most developed countries), it has also been one of the web's most basic features that DNS can be localized and run on client, LAN, provider and national services. China, for instance, runs, its own [root DNS](#) and the EU has considered the same. [Google](#) has required their [Google Public DNS](#) be used for some applications on its [Android](#) devices. Accordingly, DNS addresses / domains used for advertising may be extremely vulnerable to a broad form of ad substitution whereby a domain that serves ads is entirely swapped out with one serving more local ads to some subset of users. This is especially likely in countries, notably [Russia](#), [India](#) and [China](#), where advertisers often refuse to pay for clicks or page views. DNS-level blocking of domains for non-commercial reasons is already common in China.^[11]

3.9 AD FILTERING BY EXTERNAL PARTIES AND INTERNET PROVIDERS

Internet providers, especially mobile operators frequently offer proxies designed to reduce network traffic. Even when not targeted at ad filtering specifically these will block many types of advertisements that are too large, bandwidth consuming or otherwise deemed unsuited for the specific internet connection or target device.

4 BA.NET ADBLOCK FILTER SERVER CLOUD

BA.net Adblock DNS and VPN Filter Dedicated Server - [free demo service](#)

<http://ba.r>

Easy to use Content Filtering, Adblock and Malware Protection for Businesses of all sizes.

- Make your Internet **Faster** and Safer with free Adblock BA.net.
- Blocks Ads on any application on your network
- Blocks Malware, Tracking Sites
- Custom Corporate Blocked Sites List
- Supports iPhone on Mobile Networks using [VPN](#)
- Fully Cloud Hosted Solution
- Business Internet Monitoring and Control
- Full Technical Support, DNS Filter List Update and Monitoring Available
- Servers root access

- Adblock Administrator Manual Preview



Free On-Line Demo Service

BA.net/adblock

Adblock DNS Filter Server FlashBoot

[Free Download](#)

free Administrator Manual E-Book Preview


[Free 950k PDF](#)



Adblock and Web Security Administrator Manual E-Book. 100 Pages, 30 Illustrations, Step by Step Administration Examples

[Buy with Paypal \\$79.90](#)


Business, Library or School Security

- Custom policy blocklist
- CIPA compliance
- 2 dedicated dns filter servers
- Root access
- Unlimited devices
- \$34.99 / Month
- [Buy with PayPal](#) 



[\\$34.99 /
Month](#)

AdBlock Speed VPN iPhone

- Custom policy blocklist
- CIPA compliance
- iPhone support on mobile networks
- Android support on mobile networks
- 2 dedicated VPN filter servers
- Root access
- Unlimited devices
- \$44.99 / Month
- [Buy with PayPal](#) 

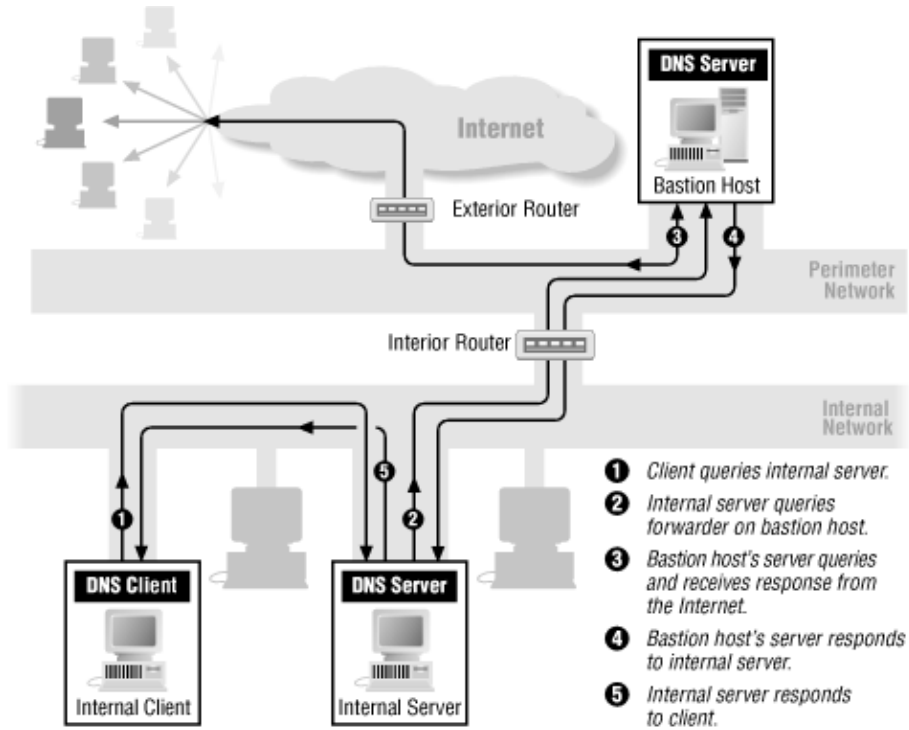


[\\$44.99 /
Month](#)

BA.net Adblock DNS Filter Server
CIPA Compliance
K12 Educational Discounts
[Contact Us adblock@ba.net](mailto:adblock@ba.net)



Contact us at 1 (206) 456-1449
adblock@ba.net



4.1 CHILDREN'S INTERNET PROTECTION ACT

4.1.1.1 Background

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

4.1.1.2 What CIPA Requires

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

(a) access by minors to inappropriate matter on the Internet;

(b) the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;

(c) unauthorized access, including so-called “hacking,” and other unlawful activities by minors online;

(d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and

(e) measures restricting minors’ access to materials harmful to them.

Schools and libraries must certify they are in compliance with CIPA before they can receive E-rate funding.

- CIPA does not apply to schools and libraries receiving discounts only for telecommunications service only;
- An authorized person may disable the blocking or filtering measure during use by an adult to enable access for bona fide research or other lawful purposes.
- CIPA does not require the tracking of Internet use by minors or adults.

You can find out more about CIPA or apply for E-rate funding by contacting the [Universal Service Administrative Company’s \(USAC\) Schools and Libraries Division \(SLD\)](#).

5.0 BA.NET ADBLOCK SPEED VPN FOR IPHONE CONFIG

1. Go to the SETTINGS



2. Go to General > VPN

●●●●○ MD MOLDCELL 12:39 77 %

[Settings](#) **General**

Restrictions On >

Date & Time >

Keyboard >

International >

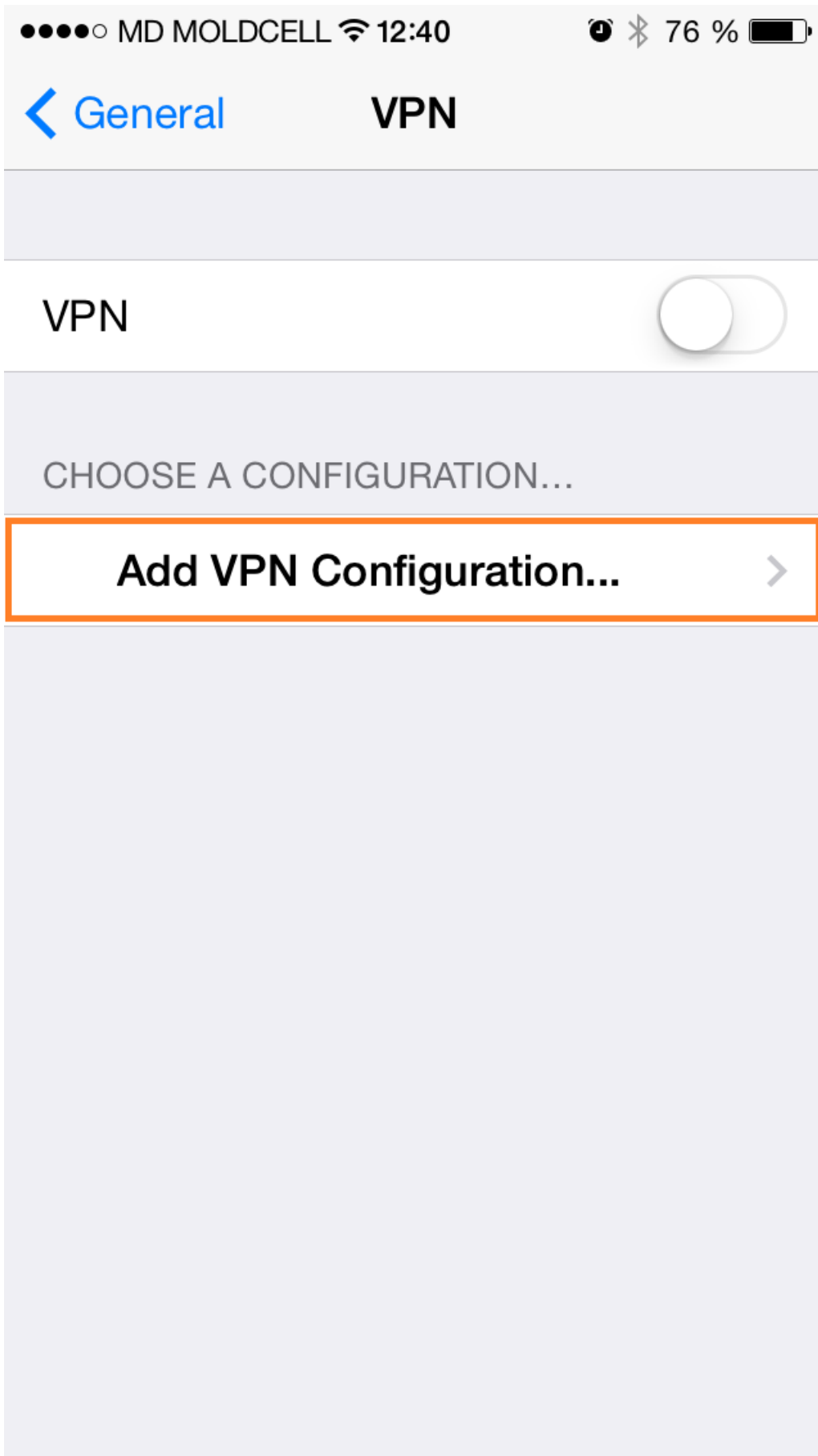
iTunes Wi-Fi Sync >

VPN Not Configured >

Profile TestFlight WebClip >

Reset >

3. Click on Add VPN Configuration



4. Select the PPTP VPN protocol at the top.
 - For Description add any name you want ex: BA.net
 - In the Server field type the vpn server name we emailed you. Example vpn12.ba.net.
 - For Account enter your VPN username.
 - For Password enter your VPN password.
 - Encryption level let it “Auto”.
 - Enable “Send All Traffic”

6. Click Save on the top right corner to save VPN configuration.

●●●● MD MOLDCELL 12:41 76 %

Cancel

Add Configuration

Save

L2TP

PPTP

IPSec

Description Required

Server Required

Account Required

RSA SecurID



Password Ask Every Time

Encryption Level

Auto >

Send All Traffic



PROXY

Off

Manual

Auto

7. You can now connect to the VPN.

To check if your IP is changed successfully open the Safari browser and go to <http://ba.net/util/geo/>.

Done. You are connected. Enjoy BA.net AdBlock VPN

4.1.2 FAQ

· Q: Do you have a solution for iPhone on Mobile Networks ?

Yes, AdBlock Speed VPN for iPhone. Speed PPTP VPN. Premium Unlimited AdBlock Servers. Available on dedicated Business Servers Only. Contact us at adblock@ba.net

· Q: Will VPN affect my mobile battery ?

Short answer no. A PPTP VPN plus BA.net Adblock DNS is the ideal way to surf faster on iPhone on mobile networks. AdBlock will speed up your connection and PPTP is the vpn protocol that will impact your battery usage the least.

PPTP is not 100% safe as an encryption protocol, but it provides adequate protection for guest hotspot surfing,

and adblock usage. The best feature of PPTP is that it is native to the iPhone, it is simple to configure and will add the least amount of overhead to your battery usage.

The AdBlock data transmission and CPU savings will combine with the low overhead of PPTP to a negligible impact on your iPhone battery.

· Q: Do you support L2PT ?

Yes, it is also available.

5 CORPORATE PROXY AUTO-CONFIG PAC

A proxy auto-config (PAC) file defines how [web browsers](#) and other [user agents](#) can automatically choose the appropriate [proxy server](#) (access method) for fetching a given [URL](#).

A PAC file contains a [JavaScript function](#) “FindProxyForURL(url, host)”. This function returns a string with one or more access method specifications. These specifications cause the user agent to use a particular proxy server or to connect directly.

Multiple specifications provide a fall-back when a proxy fails to respond. The browser fetches this PAC file before requesting other URLs. The URL of the PAC file is either configured manually or determined automatically by the [Web Proxy Autodiscovery Protocol](#).

5.1 CONTEXT

Modern web browsers implement several levels of automation; users can choose the level that is appropriate to their needs. The following methods are commonly implemented:

- Automatic proxy selection: Specify a host-name and a port number to be used for all URLs. Most browsers allow you to specify a list of domains (such as localhost) that will bypass this proxy.
- Proxy auto-configuration (PAC): Specify the URL for a PAC file with a JavaScript function that determines the appropriate proxy for each URL. This method is more suitable for laptop users who need several different proxy configurations, or complex corporate setups with many different proxies.
- [Web Proxy Autodiscovery Protocol](#) (WPAD): Let the browser guess the location of the PAC file through [DHCP](#) and [DNS](#) lookups.

5.2 PROXY CONFIGURATION

Computer [operating systems](#) (e.g., [Microsoft Windows](#), [Mac OS X](#), [Linux](#)) require a number of settings to communicate over the [Internet](#).

These settings are typically obtained from an [Internet Service Provider](#) (ISP). Either anonymous (proxy to use a [proxy server](#)) or real settings may be used to establish a network connection.

5.3 THE PAC FILE

The Proxy auto-config file format was originally designed by [Netscape](#) in 1996 for the [Netscape Navigator 2.0^{\[1\]}](#) and is a [text file](#) that defines at least one JavaScript function, FindProxyForURL(url, host), with two arguments: url is the URL of the object and host is the host-name derived from that URL. By convention, the PAC file is normally named proxy.pac. The [WPAD standard](#) uses wpad.dat.

To use it, a PAC file is published to a [HTTP server](#), and client user agents are instructed to use it, either by entering the URL in the proxy connection settings of the browser or through the use of the WPAD protocol.

Even though most clients will process the script regardless of the [MIME type](#) returned in the [HTTP reply](#), for the sake of completeness and to maximize compatibility, the HTTP server should be configured to declare the MIME type of this file to be either application/x-ns-proxy-autoconfig or application/x-javascript-config.

There is little evidence to favor the use of one MIME type over the other. It would be, however, reasonable to assume that application/x-ns-proxy-autoconfig will be supported in more clients than application/x-javascript-config as it was defined in the original Netscape specification, the latter type coming into use more recently.

A very simple example of a PAC file is:

```
function FindProxyForURL(url, host) {      return "PROXY
proxy.example.com:8080; DIRECT"; }
```

This function instructs the browser to retrieve all pages through the proxy on [port](#) 8080 of the server proxy.example.com. Should this proxy fail to respond, the browser contacts the Web-site directly, without using a proxy. The latter may fail if [firewalls](#), or other intermediary

network devices, reject requests from sources other than the proxy; a common configuration in corporate networks.

A more complicated example demonstrates some available JavaScript functions to be used in the FindProxyForURL function:

```
function FindProxyForURL(url, host) { // our local URLs from the
domains below example.com don't need a proxy:  if
(shExpMatch(host, "*.example.com")) { return
"DIRECT"; } // URLs within this network are accessed through
// port 8080 on fastproxy.example.com:  if (isInNet(host,
"10.0.0.0", "255.255.248.0")) { return "PROXY
fastproxy.example.com:8080"; } // All other requests go
through port 8080 of proxy.example.com. // should that fail to
respond, go directly to the WWW: return "PROXY
proxy.example.com:8080; DIRECT"; }
```

5.3.1 LIMITATIONS

5.3.1.1 PAC Character-Encoding

Browsers, such as [Mozilla Firefox](#) and [Internet Explorer](#), support only system default [encoding](#) PAC files, ^[citation needed] and cannot support [Unicode](#) encodings, such as [UTF-8](#).^[citation needed]

5.3.1.2 DnsResolve

The function dnsResolve (and similar other functions) performs a [DNS](#) lookup that can block your browser for a long time if the DNS server does not respond.

Caching of proxy auto-configuration results by domain name in Microsoft's [Internet Explorer](#) 5.5 or newer limits the flexibility of the PAC standard. In effect, you can choose the proxy based on the domain name, but not on the path of the URL. Alternatively, you need to disable caching of proxy auto-configuration results by editing the [registry](#), a process described by de Boyne Pollard (listed in [further reading](#)).

It is recommended to always use [IP addresses](#) instead of host domain names in the isInNet function for compatibility with other Windows

components which make use of the Internet Explorer PAC configuration, such as [.NET 2.0 Framework](#). For example,

```
if (isInNet(host, dnsResolve(sampledomain), "255.255.248.0")) // .NET 2.0 will resolve proxy properly
if (isInNet(host, sampledomain, "255.255.248.0")) // .NET 2.0 will not resolve proxy properly
```

The current convention is to fail over to direct connection when a PAC file is unavailable.

Shortly after switching between network configurations (e.g. when entering or leaving a VPN), dnsResolve may give outdated results due to DNS caching.

For instance, Firefox usually keeps 20 domain entries cached for 60 seconds. This may be configured via the network.dnsCacheEntries and network.dnsCacheExpiration configuration variables. Flushing the system's [DNS cache](#) may also help, which can be achieved e.g. in Linux with `sudo service dns-clean start`.

5.3.1.3 myIpAddress

The myIpAddress function has often been reported to give incorrect or unusable results, e.g. 127.0.0.1, the IP address of the localhost. It may help to remove on the system's host file (e.g. /etc/hosts on Linux) any lines referring to the machine host-name, while the line 127.0.0.1 localhost can, and should, stay.

On Internet Explorer 9, isInNet("localhostName", "second.ip", "255.255.255.255") returns true and can be used as a workaround.

The myIpAddress function assumes that the device has a single IPv4 address. The results are undefined if the device has more than one IPv4 address or has IPv6 addresses.

5.3.1.4 Security

In 2013, researchers began warning about the security risks of proxy auto-config.^[2] The threat involves using a PAC to redirect the victim's browser traffic to an attacker-controlled server instead.

5.3.1.5 Others

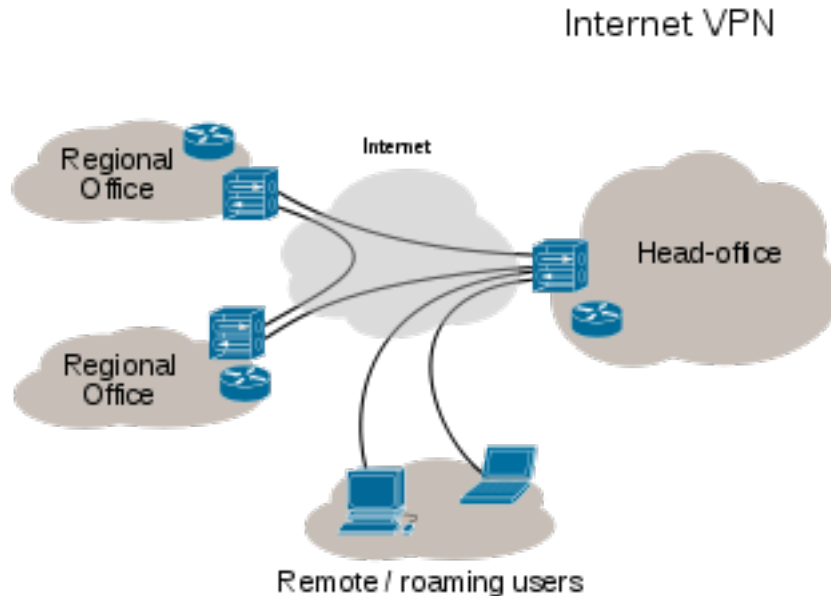
Further limitations are related to the [JavaScript engine](#) on the local machine.

5.3.2 ADVANCED FUNCTIONALITY

More advanced PAC files can reduce load on proxies, perform load balancing, fail over, or even [black/white listing](#) before the request is sent through the network. One can return multiple proxies:

```
return "PROXY proxy1.example.com:8080; PROXY  
proxy2.example.com:8080";
```

6 BA.NET ADBLOCK SPEED VPN FOR IPHONE



6.1 VPN CONNECTIVITY OVERVIEW

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the public network.^[1] A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. Major implementations of VPNs include OpenVPN and IPsec.

A VPN connection across the Internet is similar to a wide area network (WAN) link between websites. From a user perspective, the extended network resources are accessed in the same way as resources available