I wrote an IPFire Security Hardening guide

I wrote an IPFire Security Hardening guide

by **dnl** » October 30th, 2015, 9:35 am

dnl — Posts: 375 — Joined: June 28th, 2013, 11:03 am

Hello,

I'd appreciate feedback, good or bad, from experienced users on a new IPFire Security Hardening page I wrote in the wiki:
https://wiki.ipfire.org/optimization/st ... _hardening

It took me a lot of time to put together, so unlike most wiki pages, I ask that you please do not make changes directly to it just yet. Please start a discussion in this thread first and when the page is fully developed it will be open for normal changes.

Things to note:

1. I added the implementation scale so that the page would not be too overwhelming for new users. As I have emphasised on the page it is *subjective*. So if you really feel I've incorrectly rated something please give a good reason why. Security is all about context, so by adding a scale for everybody I've had to compromise and make some assumptions.

2. You may have more ideas for security hardening, which is great! When the discussion has died down here we may need to remove some of the items so that the list is not too long and overwhelming (it possibly already is?).

3. It would be awesome if in future some of these items could be on by default in a new IPFire install (where possible)

4. I'd love to add some helpful security quotes (not too many though) and another image if anybody has an appropriate one.

Thanks to twilson who discovered the isolated page before it was ready and added a little helpful input.

Thanks!

EDIT: Updated link to Wiki after change in Wiki structure

Last edited by **dnl** on December 2nd, 2018, 6:02 am, edited 1 time in total.

Re: I wrote an IPFire Security Hardening guide

by **bloater99** » October 30th, 2015, 2:36 pm

bloater99 — Posts: 482 — Joined: October 13th, 2014, 3:47 pm

I appreciate your time and effort. I will read through it as soon as I am able and provide some feedback.

As I give feedback, I'll just edit this post to put in.
1) under log checking by Country, you might want to consider that GeoIP Block will affect this. For example, I block all countries except my own, so the Fw-Loggraphs (Country) section only shows firewall hits from my own country. To see which countries attack most frequently, go to Firewall->iptables->iptables:GEOIPBLOCK <Update>.

2) In the squidclamav section, you may want to reference recent tests conducted by av-test.org which show clamav detection rates at 15% for Windows malware and 66% for linux malware:
https://www.av-test.org/en/news/news-si ... -the-test/

IPFire - An open source firewall solution
IPFire 2.25 - Core Update 153 on x86_64
Intel Atom 330 @ 1.60GHz x2 - 2GB

Re: I wrote an IPFire Security Hardening guide

by **dnl** » November 1st, 2015, 9:59 am

dnl — Posts: 375 — Joined: June 28th, 2013, 11:03 am

> **bloater99 wrote:**
> I appreciate your time and effort. I will read through it as soon as I am able and provide some feedback.

Thanks!

> **bloater99 wrote:**
> 1) under log checking by Country, you might want to consider that GeoIP Block will affect this. For example, I block all countries except my own, so the Fw-Loggraphs (Country) section only shows firewall hits from my own country. To see which countries attack most frequently, go to Firewall->iptables->iptables:GEOIPBLOCK <Update>.

Hmm. Blocking all countries but your own only works if you're in the USA and don't deal much with overseas software or companies. I'm still a bit surprised though. Isn't this forum and wiki hosted in Germany? If so have you had to add an exemption for it?

In the "Use GeoIP Block" recommendation I deliberately did not name any countries, even though there are some obvious ones with a high percentage of malicious traffic.

Anyway thanks for the input! I've added it to the log check section - hopefully it's what you were after.

> **bloater99 wrote:**
> 2) In the squidclamav section, you may want to reference recent tests conducted by av-test.org which show clamav detection rates at 15% for Windows malware and 66% for linux malware:
> https://www.av-test.org/en/news/news-si ... -the-test/

Awesome thanks, I hadn't found a link like that!
Wow, that's exceptionally bad, I hadn't realised it was as low as 15% for Windows malware!! It's probably not worth turning on if you have a low-power IPFire system, given most networks (sadly) tend to have a heavy use of Microsoft operating systems (or so I have assumed in writing this guide anyway).

Thanks for your help!

Re: I wrote an IPFire Security Hardening guide

by **ummeegge** » November 1st, 2015, 10:17 am

ummeegge — Community Developer — Posts: 5001 — Joined: October 9th, 2010, 10:00 am

Hi all,
at a first, thanks dnl for your hard work to start with a guide like this i think it is a very good idea.

Some suggestions for the second:
- SSH Pubkey authentication might be good to mention.
- The firewall policies (especially FORWARD block) serves also a good way fo a better protection cue "Everything is forbidden that is not explicitly allowed" e.g. in combination with Squids conventional mode.
- OpenVPN for WLAN. ACCEPT rule for tun+ only.
- rkhunter can be installed with a simple "./installer.sh --install" (shell script installer and Perl).
- Ossec is unofficially available for IPFire --> https://forum.ipfire.org/viewtopic.php? ... 924#p80449 <-- if there are more testings results/feedback from people it may become a candidate for IPfire ?!
- With Portspoof it is the same --> http://portspoof.org/ --> https://forum.ipfire.org/viewtopic.php? ... 399#p83755 <-- cue use NON IANA definitions to WAN and DNAT it to origin if possible.

Some thoughts from here.

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: I wrote an IPFire Security Hardening guide

by **dnl** » November 1st, 2015, 10:28 am

dnl — Posts: 375 — Joined: June 28th, 2013, 11:03 am

Replying to a post from ummeegge which I believe was meant to be in this thread instead

> **ummeegge wrote:**
> - Ossec is unofficially available for IPFire --> https://forum.ipfire.org/viewtopic.php? ... 924#p80449 <-- if there are more testings results/feedback from people it may become a candidate for IPfire ?!

I hadn't seen that!! More things to try when I've got more time 🤓
Thank you! I've now significantly updated the "Use TripWire" section to "Use a Host-Based Intrusion Detection System" and mentioned your OSSEC version. Please let me know if it's good.

> **ummeegge wrote:**
> - SSH Pubkey authentication might be good to mention.

Yes true. Are you suggesting that people should use it in addition to a password or instead of? I'll add this when I have time later this week.

> **ummeegge wrote:**
> - The firewall policies (especially FORWARD block) serves also a good way for a better protection cue "Everything is forbidden that is not explicitly allowed" e.g. in combination with Squids conventional mode.

Sorry, I'm not sure what you mean by this! Could you please explain?

The three "firewall policies" on the "Firewall Options" WUI page already default to the "DROP" setting don't they? If so what are you hoping to add, please?

> **ummeegge wrote:**
> - OpenVPN for WLAN. ACCEPT rule for tun+ only.

I'm afraid that I do not understand this either. Could you please explain more?

> **ummeegge wrote:**
> - rkhunter can be installed with a simple "./installer.sh --install" (shell script installer and Perl).

Yes good point! Perhaps we (me if I have time, but anybody else can too!) should write another wiki page explaining how to install it and how to use it with IPFire's new "Mailservice"? 🙂
Thanks for this - I will update the Security Hardening page with this soon (this week).

> **ummeegge wrote:**
> - With Portspoof it is the same --> http://portspoof.org/ --> https://forum.ipfire.org/viewtopic.php? ... 399#p83755 <-- cue use NON IANA definitions to WAN and DNAT it to origin if possible.

Wow, you are giving me a lot of good things to research! I've not heard of portspoof but it sounds excellent. I don't want you to have to translate a whole post in that thread, but could you please give a brief summary of that thread? (I can't read German) Are people using portspoof with IPFire?

Thank you for all this!

Re: I wrote an IPFire Security Hardening guide

by **dnl** » November 1st, 2015, 10:43 am

dnl — Posts: 375 — Joined: June 28th, 2013, 11:03 am

Thanks to **ummeegge**, I've just added an "Install Rootkit Hunter" section to the page.
A separate page with instructions on how to install rkhunter on a shell and integrate with fcron will need to be written.

For now I have given this an impact of "significant" (as rkhunter is pretty helpful but I'm not sure it's worthy of a "major" security benefit tag?) and an effort to implement of "medium" because it requires usage of the shell (it is not just a simple GUI addon)

I am beginning to wonder if the security hardening guide is becoming too long now! Wow it's got a lot of things in it. Hopefully the implementation scale helps people decide which parts they will spend the time and effort to do.

Re: I wrote an IPFire Security Hardening guide

by **ummeegge** » November 1st, 2015, 5:01 pm

ummeegge — Community Developer — Posts: 5001 — Joined: October 9th, 2010, 10:00 am

Hi dnl,

> **dnl wrote:**
> Replying to a post from ummeegge which I believe was meant to be in this thread instead

yeah sorry this was my bad, had a lot of open windows and accidentially wrote into the wrong thread 😳 , have fixed that.

> **dnl wrote:**
> Thank you! I've now significantly updated the "Use TripWire" section to "Use a Host-Based Intrusion Detection System" and mentioned your OSSEC version. Please let me know if it's good.

Looks good.

> **dnl wrote:**
> Yes true. Are you suggesting that people should use it in addition to a password or instead of? I'll add this when I have time later this week.

I meant instead of. I think both isn´t possible.

> **dnl wrote:**
> Sorry, I'm not sure what you mean by this! Could you please explain?
>
> The three "firewall policies" on the "Firewall Options" WUI page already default to the "DROP" setting don't they? If so what are you hoping to add, please?

No problem. The section "Default firewall behaviour" describes it in the wiki what i mean -->
http://wiki.ipfire.org/en/configuration ... ult-policy . If you block the FORWARD chain (all ports are closed also for the outgoing traffic) you need to set rules for every connection which is at the first more work but it makes sense in my opinion cause you only allow traffic which you accepted before and you get a better know how of your network needs, GeoIP ruleset could also be useful in that case. In combination with a NON-transparent proxy with authentication regulates this way also in another aspect.

> **dnl wrote:**
>
> > **ummeegge wrote:**
> > - OpenVPN for WLAN. ACCEPT rule for tun+ only.
>
> I'm afraid that I do not understand this either. Could you please explain more?

OpenVPN provides authentication via certificates so no passwords anymore. In that way it is possible to write your own IPTables rule for the tun interface only so there is no need for a MAC filter anymore (no passwords, authentication via certificates, strong encryption, PFS, traffic over UDP protocol {could be faster}, ...) May this is a little too hacky for regular users but nevertheless i wanted to mention it.

> **dnl wrote:**
> I've not heard of portspoof but it sounds excellent. I don't want you to have to translate a whole post in that thread, but could you please give a brief summary of that thread? (I can't read German) Are people using portspoof with IPFire?

Yes sure. There are different operating modes in Portspoof which would sprinkle the frame here to explain them in detail but as a short one. If e.g. an Nmap scan starts to investigate infos about your system (first step in attacking mode is regular info investigation), Portspoof delivers in the first step that all ports are open (open port mode), if the NSE scripts in Nmap starts, Portspoof delivers false signatures and payloads (Portspoof provides over 8000 regular signatures). As a possible third step it could becomes also unpleasant for possible attackers cause Portspoof is also able to deliver exploits <-- attention with this, in germany you can belong to the §303b . So Portspoof is not only a service emulator but also a frontend exploitation framework.
We have tested it relativley extensive and sure not only myself uses it in regular. The linked topic provides an in- uninstaller, automatic firewall integration and some other things, all comments are hold in english so you should be able to understand it a little better. For more infos take a look in here --> http://www.linux-magazine.com/Online/Fe ... -Portspoof . If you´d like to start also some testings, start a new topic for this theme in english section will hang on then.

> **dnl wrote:**
> Wow, you are giving me a lot of good things to research!Thank you for all this!

You are welcome, happy that you can use it 🙂 .

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: I wrote an IPFire Security Hardening guide

by **H&M** » November 3rd, 2015, 7:45 am

H&M — Posts: 471 — Joined: May 29th, 2014, 9:38 pm — Location: Europe

Hi,

I always think that traffic has:
1. 2 directions - in & out
2. Coming from a FQDN (going to an FQDN) and from an IP.

Therefore:
a. If you decide to use GeoIP to filter access from "bad countries", I do recommend to create a FW group for those countries and block also the exit toward these countries. In my case: I block traffic from ALL countries except mine (incoming) and allow exit traffic for only a few countries. Bad side: in one day my Windows stations got as update.microsoft.com an IP from one of blocked countries (instead of local cached copy) and updates failed. For a week - until DNS returned local cached copy!

b. Blocking one IP range (a country) is useless: most of large providers (and I include here also the large botnets) have points of presence in several countries. You need to fight against that at FQDN level: if you block DE IP range for example, than I do recommend to block also .DE DNS TLD! As I said: for both directions: in and out!
Yes, this might sound too much, but wait: do this for all parked domains, dynamic domains or domains for countries that no longer exists! Example: former Iugoslavia, Former Soviet Union domains are still available and I hosts some sites using IPs from all around the IP range! And, of course, block all requests for domains being known as botnets/malware domains.

For that you need an secure DNS provider that allows you to filter your DNS requests based on categories. I use OpenDNS.

I've blocked: in traffic from all the IPs ranges in the world except my country and out traffic toward IP ranges from CN, RU, SU, PW and other countries I should never go with my traffic (Africa for example). I've also blocked the TLD domains CN, RU, SU and some dynamic domains - in both directions! I've blocked all malware domains, advertisers, tracking domains.
I've blocked a large range of IPs from Yahoo - one single IP from this range had more than 27000 registered domains on that IP!

Is is very handy also when I watch Tv over IP TV: I don't get traffic from unwanted areas.

As result, I've saw in my logs some interesting traffic being stopped:
a) One major newspaper redirected me to an African country IP. The traffic was blocked.
b) Some of my phones tried to reach IPs from CN and did DNS queries for CN domains (Baidu software on my newly bought Android, Android delivered in Europe 😛)
c) Update.windows.com was resolver to an IP from a very distant country. This traffic was stopped.
d) more that 200 hits per day for trackers or advertisers that try to create a digital profile based on the sites I've accessed. All this traffic is blocked at DNS level by OpenDNS (I see that in the OpenDNS dashboard).

As result my phones and smartTV do not display anymore advertise about "you got a virus, clean yor phone", and my SmartTV stopped traying to reach some Asian IPs without any reverse DNS registered to it (I've checked that IP using domaintools.com).

Now I have quiet in my small network!

It will be very useful to have a full list of IpFire mirrors and do a special FW list for the FW (kernel) to allow traffic only to the following sites/IPs:
1. The NTP servers
2. The DNS servers
3. The whois servers
4. The mirror servers (used by pakfire)
5. The URL firlter, Snort and other add-on update sites.

And then block everything else.
Firewall itself should be hardened as tough as possible.

Thank you,
H&M

Re: I wrote an IPFire Security Hardening guide

by **dnl** » November 3rd, 2015, 9:01 am

dnl — Posts: 375 — Joined: June 28th, 2013, 11:03 am

Thanks H&M! I'll respond to your suggestions soon.

About SSH key authentication

> **ummeegge wrote:**
>
> > **dnl wrote:**
> > Yes true. Are you suggesting that people should use it in addition to a password or instead of?
>
> I meant instead of. I think both isn´t possible.

Although it may not be with the IPFire WUI, it is most definitely an option with OpenSSH. Check the
"AuthenticationMethods" section of the sshd_config man page.
(I used to do this way back when I actually had SSH open on my internet connection some years ago).

Sadly keys are usually not considered two-factor authentication, because if somebody knows your password they will also have access to your keys. The only exception would be if you had a key with a strong passphrase, but it seems to me that most people don't.

> **ummeegge wrote:**
> No problem. The section "Default firewall behaviour" describes it in the wiki what i mean -->
> http://wiki.ipfire.org/en/configuration ... ult-policy . If you block the FORWARD chain (all ports are closed also for the outgoing traffic) you need to set rules for every connection which is at the first more work but it makes sense in my opinion cause you only allow traffic which you accepted before and you get a better know how of your network needs, GeoIP ruleset could also be useful in that case. In combination with a NON-transparent proxy with authentication regulates this way also in another aspect.

Yes OK. I don't know why I didn't think of that!
It's a "Major" security benefit but also "high" effort to implement. I'll try to write this up soon.

> **ummeegge wrote:**
> **OpenVPN for WLAN. ACCEPT rule for tun+ only.**
> OpenVPN provides authentication via certificates so no passwords anymore. In that way it is possible to write your own IPTables rule for the tun interface only so there is no need for a MAC filter anymore (no passwords, authentication via certificates, strong encryption, PFS, traffic over UDP protocol {could be faster}, ...) May this is a little too hacky for regular users but nevertheless i wanted to mention it.

No that's a good point. Assuming strong certificates are generated and they are shared in a secure way this does sound better than password-based authentication. We might want to add a section about VPN hardening?

About portspoof

> **ummeegge wrote:**
> We have tested it relativley extensive and sure not only myself uses it in regular. The linked topic provides an in- uninstaller, automatic firewall integration and some other things, all comments are hold in english so you should be able to understand it a little better. For more infos take a look in here --> http://www.linux-magazine.com/Online/Fe ... -Portspoof . If you´d like to start also some testings, start a new topic for this theme in english section will hang on then.

I really like the idea of portspoof (it's cool!), but the more I think about it the more I would avoid recommending it for security hardening. The reason is that it makes your IP suspicious.

In my opinion you want your internet connection to be as common as possible (to not stand out). While using portspoof might cause trouble for a script kiddy, it could also draw the attention of a much more skilled hacker/cracker.

If you think it's still a real benefit, I'm happy to add it, but I would want to add a warning box explaining what I have just said. What do you think?

Thanks again ummeegge!

edit - adding link to copy of sshd_config man page which has AuthenticationMethods

Re: I wrote an IPFire Security Hardening guide

by **H&M** » November 3rd, 2015, 8:05 pm

H&M — Posts: 471 — Joined: May 29th, 2014, 9:38 pm — Location: Europe

Hi dnl,

Second aspect I want to raise: management of IpFire.
In my previous post I've touched only the external network.

Now I want to bring in attention the LAN & Management of IpFire. How to protect the box for attacks from inside the LAN.

Recommendations:
1. Do use Guardian.
2. Set it to block any wrong attempt to loging on SSH or Web GUI. Set it to "paranoid" - at second wrong attempt block that internal IP
3. Use "management IP range" - create FW rules to allow management of IpFire only from that limited range of IPs.
4. Above are not enough: the best security is at Layer 1: physical layer! If you have multiple eth cards connected to LAN, create FW rules to accept SSH traffic only to a dedicated eth and keep it connected to a single machine, machine that is kept powered down if you don't intend to do IpFire management. Power up this management machine only when you need it.
5. The strongest solution: If you have the possibility to do management from Serial Console - stop sshd and httpd service and keep them stopped and start them over serial console only when you need them

These days I've reach the level described in point 4: remote management services are shut down.
I have a dedicated laptop (that will be replaced with an RaspBerry Pi in the future) connected over serial console to IpFire.
This laptop is used just to launch sshd & httpd when I need to manege IpFire box.
This idea is very old: Cisco created some Terminal Servers that allowed us to manage Cisco boxes only over serial console and keep telnet/ssh services down. I've just replicated this experience with IpFire
The laptop is on halt (powered down) and is awaken only when I need to manage the IpFire box. In this way any attack against IpFire is useless: the box is kept with management services in down state.

Las, but not least: create backups and keep them safe, outside of the IpFire machine.
Anytime you should be able to check the configuration changes and be able to restore them fast.

For this, I've build an NFS server (also based on IpFire) and all backups are dumped to this NFS server.
The server is always powered down, each IpFire knows how to wake it when the backup need to be run via schedule.
After the backup, the NFS backup server goes to down state again in order to be protected from any attacks.

Best,
H&M

Re: I wrote an IPFire Security Hardening guide

by **dnl** » November 4th, 2015, 7:10 am

dnl — Posts: 375 — Joined: June 28th, 2013, 11:03 am

Hey H&M thanks for your input!

> **H&M wrote:**
> a. If you decide to use GeoIP to filter access from "bad countries", I do recommend to create a FW group for those countries and block also the exit toward these countries. In my case: I block traffic from ALL countries except mine (incoming) and allow exit traffic for only a few countries. Bad side: in one day my Windows stations got as update.microsoft.com an IP from one of blocked countries (instead of local cached copy) and updates failed. For a week - until DNS returned local cached copy!
>
> b. Blocking one IP range (a country) is useless: most of large providers (and I include here also the large botnets) have points of presence in several countries. You need to fight against that at FQDN level: if you block DE IP range for example, than I do recommend to block also .DE DNS TLD! As I said: for both directions: in and out!
> Yes, this might sound too much, but wait: do this for all parked domains, dynamic domains or domains for countries that no longer exists! Example: former Iugoslavia, Former Soviet Union domains are still available and I hosts some sites using IPs from all around the IP range! And, of course, block all requests for domains being known as botnets/malware domains.
>
> For that you need an secure DNS provider that allows you to filter your DNS requests based on categories. I use OpenDNS.
>
> I've blocked: in traffic from all the IPs ranges in the world except my country and out traffic toward IP ranges from CN, RU, SU, PW and other countries I should never go with my traffic (Africa for example). I've also blocked the TLD domains CN, RU, SU and some dynamic domains - in both directions! I've blocked all malware domains, advertisers, tracking domains.
> I've blocked a large range of IPs from Yahoo - one single IP from this range had more than 27000 registered domains on that IP!
>
> Is is very handy also when I watch Tv over IP TV: I don't get traffic from unwanted areas.
>
> As result, I've saw in my logs some interesting traffic being stopped:
> a) One major newspaper redirected me to an African country IP. The traffic was blocked.
> b) Some of my phones tried to reach IPs from CN and did DNS queries for CN domains (Baidu software on my newly bought Android, Android delivered in Europe 😛)
> c) Update.windows.com was resolver to an IP from a very distant country. This traffic was stopped.
> d) more that 200 hits per day for trackers or advertisers that try to create a digital profile based on the sites I've accessed. All this traffic is blocked at DNS level by OpenDNS (I see that in the OpenDNS dashboard).
>
> As result my phones and smartTV do not display anymore advertise about "you got a virus, clean yor phone", and my SmartTV stopped traying to reach some Asian IPs without any reverse DNS registered to it (I've checked that IP using domaintools.com).
>
> Now I have quiet in my small network!

I agree that blocks need to be in both directions and will try to think of how that can be added to the page. Do you have any suggestions? (Have you read the page in detail yet? Sadly It's already quite long!)

I'm afraid I partly disagree with you on blocking domain names. Blocking IPs based on their geographic location is different to blocking IPs based on their domain name.

For example, I choose to block IPs belong to China because;
1. The whole country has a very high percentage of malicious traffic compared with non-malicious traffic
2. Nobody on my network needs to communicate directly with China (no business reason, no friends or family for example) - so all traffic from the country is "unwanted"

Despite the good example you gave with Windows Update, I generally don't care about blocking .cn domains though. As you've said they can be registered from anywhere in the world. Often people use domain names just because they like the FQDN! Look at Tuvalu (.tv) or the Federated States of Micronesia (.fm)! People don't actually host servers in those small countries.

I am fully aware that blocking China does protect me from Chinese hackers who use botnets or compromised boxes in other countries. However by just blocking their geographic IPs I can significantly reduce malicious traffic to my network - which also reduces the number of hits against my IDS, making it easier to see more dangerous attacks. I think we both agree on that though.

Using OpenDNS is a good suggestion for security, but I'd want to note that you are sacrificing your privacy to do so. I'll add this somewhere to the page.
(I think it's sad that Cisco bought them as things will change)

> **H&M wrote:**
> It will be very useful to have a full list of IpFire mirrors and do a special FW list for the FW (kernel) to allow traffic only to the following sites/IPs:
> 1. The NTP servers
> 2. The DNS servers
> 3. The whois servers
> 4. The mirror servers (used by pakfire)
> 5. The URL firlter, Snort and other add-on update sites.
>
> **And then block everything else.**
> **Firewall itself should be hardened as tough as possible.**

Yeah, that would be handy. I've noticed that IPFire uses mirrors in some countries I block. (I'm sure there are honest people in those countries using IPFire who suffer through more attacks than I often do though.)

Through the process of writing this I've come to the conclusion that while IPFire is already very good, it could be more hardened by default. I hope that this conversation and the wiki page are noticed by the key developers who have control over the high-level design.

Thanks again, this has been a good discussion.
I'll get to your next reply soon (ran out of time now)!

Re: I wrote an IPFire Security Hardening guide

by **dnl** » November 4th, 2015, 7:17 am

dnl — Posts: 375 — Joined: June 28th, 2013, 11:03 am

I just remembered another reason why blocking top-level-domains is actually important. It's not Geographic location, but newness!

The new TLDs released in the past year have a very high percentage of malicious sites:
https://www.bluecoat.com/company/press- ... August2015

Re: I wrote an IPFire Security Hardening guide

by **H&M** » November 4th, 2015, 10:10 pm

H&M — Posts: 471 — Joined: May 29th, 2014, 9:38 pm — Location: Europe

> **dnl wrote:**
> Hey H&M thanks for your input!
>
> I agree that blocks need to be in both directions and will try to think of how that can be added to the page. Do you have any suggestions? (Have you read the page in detail yet? Sadly It's already quite long!)

Hi dnl,
Yes I have one:

Look here - it also include print screens: viewtopic.php?f=52&t=11950&p=83417#p83579
Note: below that post is also a correction - I used SQUID therefore the source of traffic is the FW (black network) and not Green. If you don't use SQUID then source is GREEN or Blue (depending where your client / computer is connected).

Yes I have read it.
It is, as you already pointed out, quite long.
I will think to a structure - some groups to gather them toghether. But later, now is very late in my country.

> **dnl wrote:**
> I'm afraid I partly disagree with you on blocking domain names. Blocking IPs based on their geographic location is different to blocking IPs based on their domain name.

Well, my intention **was to block dynamic domains**, and later I've added to this blocking list the known "attackers" (like China, Rusia) and domains for countries that no longer exists. Like SU (Soviet Union).

Have a look here: I've discovered one IP from USA , registered to Yahoo!!! that has more than 227000 domains associated with than IP!!
viewtopic.php?f=52&t=11248&start=30#p81517

Picture with that IP:
download/file.php?id=170

I do believe that blocking dynamic domains should be put as recommendation.

By the way: do you know any method to discover the TLD used by DDNS? Like .biz, no-ip.org, etc?

Why I am asking this:
I know that FBI stopped in the past several botnets that used also servers bought from legit cloud providers from Germany and USA (as a matter of fact some of the IPs of these providers are registered in SNORT rules - and trigger alerts with the name of that cloud services provider - have a look at sid:2016995: "ET TROJAN Connection to 1&1 Sinkhole IP (Possible Infected Host)" - it blocks Ip 212.227.20.19).
All these botnets used dynamic domains and from that article I've started to search for a way to block multiple domains when a DNS query is launched. And then I've discovered OpenDNS...

Best,
H&M

Re: I wrote an IPFire Security Hardening guide

by **dnl** » November 7th, 2015, 11:27 pm

dnl — Posts: 375 — Joined: June 28th, 2013, 11:03 am

Hello again,

Thanks for your reply H&M, I'll add something about blocking domains when I have time (I've not had as much time as I expected).

No, I'm not sure how to block the domain names registered to dynamic DNS providers - that's a good point.

Re: I wrote an IPFire Security Hardening guide

by **ummeegge** » November 9th, 2015, 7:02 pm

ummeegge — Community Developer — Posts: 5001 — Joined: October 9th, 2010, 10:00 am

Hi all,

> **dnl wrote:**
> Although it may not be with the IPFire WUI, it is most definitely an option with OpenSSH. Check the
> "AuthenticationMethods" section of the sshd_config man page.
> (I used to do this way back when I actually had SSH open on my internet connection some years ago).

Yes wright the WUI do not delivers this but altough a script is available in the wiki which should do this with a little more automation --> http://wiki.ipfire.org/en/configuration/system/ssh but i hadn´t used it may cause it is one of the first things i do on new machines (commands are presant ;-) .

> **dnl wrote:**
> Sadly keys are usually not considered two-factor authentication, because if somebody knows your password they will also have access to your keys. The only exception would be if you had a key with a strong passphrase, but it seems to me that most people don't.

therefor you need to belong to the admin machine (incl. the key password protection) and may in someways a better possibility as an password only based alternate access which provides the FW itself?!

> **dnl wrote:**
> We might want to add a section about VPN hardening?

This is a great idea, there are a lot of examples findable in the forum and also in the wiki but apart from that, OpenVPN 2.4.x will deliver also some new stuff may also ECC crypto, will see. So if you want to start a topic may first in the forum for a discussion in that topic, great 🙂 .

> **dnl wrote:**
> I really like the idea of portspoof (it's cool!), but the more I think about it the more I would avoid recommending it for security hardening. The reason is that it makes your IP suspicious.
>
> In my opinion you want your internet connection to be as common as possible (to not stand out). While using portspoof might cause trouble for a script kiddy, it could also draw the attention of a much more skilled hacker/cracker.

You are absolutly right, see it more as an possibility for forensic, while attacking time or simply as an new idea of how an active response could work too (a little marketing is also in 😊).

> **dnl wrote:**
> If you think it's still a real benefit, I'm happy to add it, but I would want to add a warning box explaining what I have just said. What do you think?

If your time is more generous to you, what are you thinkin to start simply our own research on that topic ? Experience may come also by more usage/more time in the german section and we can bring it all together ?! Let´s see.

> **dnl wrote:**
> Thanks again ummeegge!

You are welcome, i thank you too 🙂 .

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

I wrote an IPFire Security Hardening guide

Re: I wrote an IPFire Security Hardening guide

by **FischerM** » November 15th, 2015, 12:24 pm

FischerM
Community Developer
Posts: 1025
Joined: November 2nd, 2011, 12:28 pm

Hi,

@dnl:

Perhaps you'd like to add privoxy to the section "2. Additional configuration"?

I got it running for about 6 months now without problems.

Jm2c – best,
Matthias

Re: I wrote an IPFire Security Hardening guide

by **dnl** » January 15th, 2016, 11:25 pm

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

> **FischerM wrote:**
> Hi,
>
> @dnl:
>
> Perhaps you'd like to add privoxy to the section "2. Additional configuration"?
>
> I got it running for about 6 months now without problems.
>
> Jm2c – best,
> Matthias

Hello,

I only just read your reply. Thanks for the suggestion, I will investigate 'provixy' as I hadn't heard of it before!

Please feel free to add things to the page now as you see fit.
In December I removed the statement at the beginning of the page saying that I was working on it.

Thanks for that!

Re: I wrote an IPFire Security Hardening guide

by **dnl** » January 15th, 2016, 11:29 pm

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

I guess the only issue is that the page is already too long for the target audience. That is, people who are new to IPFire and wish to perform extra security hardening.

It would be helpful if every suggestion on the page had clear instructions for implementation in the same language as the Wiki (even if those instructions are on a separate, but linked page). Unfortunately your link for privoxy is to the German forum and many of us can't read German. 😟

Re: I wrote an IPFire Security Hardening guide

by **FischerM** » January 16th, 2016, 7:34 am

FischerM
Community Developer
Posts: 1025
Joined: November 2nd, 2011, 12:28 pm

Hi,

> **dnl wrote:**
> ...Unfortunately your link for privoxy is to the German forum and many of us can't read German

This should be no problem. I wrote the linked posting for the german forum, I can write a "condensed" version in english for the wiki... 😉

Best,
Matthias

Re: I wrote an IPFire Security Hardening guide

by **dnl** » January 22nd, 2016, 8:37 am

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

> **FischerM wrote:**
> This should be no problem. I wrote the linked posting for the german forum, I can write a "condensed" version in english for the wiki... 😉

Excellent! Thanks for that!

I've not had much time lately, but PM me when it is done if I can help you by reviewing it.

Re: I wrote an IPFire Security Hardening guide

by **liukuohao** » October 18th, 2016, 4:12 am

liukuohao
Posts: 76
Joined: June 17th, 2013, 4:16 am

Hello dnl,

By default a firewall will allow any traffic initiated from the GREEN network to access the RED without restriction.
If in case, any of the client in the GREEN network is compromised, and start pouring out information unknowingly to the attacker located on outside your network.

Would it be advisable.....
Configure 1st firewall rule.....
Configure 2nd firewall rule.....
Configure 3rd firewall rule....etc...etc.....
to have a LAST firewall rule- REJECT all other traffic?

Re: I wrote an IPFire Security Hardening guide

by **dnl** » October 19th, 2016, 3:07 am

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

> **liukuohao wrote:**
> Hello dnl,
>
> By default a firewall will allow any traffic initiated from the GREEN network to access the RED without restriction.
> If in case, any of the client in the GREEN network is compromised, and start pouring out information unknowingly to the attacker located on outside your network.
>
> Would it be advisable.....
> Configure 1st firewall rule.....
> Configure 2nd firewall rule.....
> Configure 3rd firewall rule....etc...etc.....
> to have a LAST firewall rule- REJECT all other traffic?

Hello liukuohao,
Thank you for your suggestion!

Are you suggesting that the security guide should recommend outbound firewall rules, instead of the default "allow all"? Is that right?

If so I agree that this does improve security, but there needs to be instructions on how to define these rules for a network. Outbound rules can be quite complex, unless you have a simple network.

Re: I wrote an IPFire Security Hardening guide

by **liukuohao** » October 19th, 2016, 3:56 am

liukuohao
Posts: 76
Joined: June 17th, 2013, 4:16 am

Yes, something like that. Allow what is required to flow out (for example, http, https, dns.....etc....etc)
So, at the top of firewall rule, you ALLOW traffic http, https, dns.....etc.....etc.
then at the very last rule, BLOCK all other traffic flowing out from GREEN network to RED.
If say, a PC in the GREEN network got infected with BOTNET, then it will not able to communicate to its HOST living outside in the RED /WAN network. Just a suggestion only. 😃

Over in pfSense, the people always preach us not to use Default Allow rule.
Allow what kind of traffic (http, https, dns, ftp...etc) is necessary for your PC GREEN network to work with.
Block what is not required.

Re: I wrote an IPFire Security Hardening guide

by **liukuohao** » October 19th, 2016, 7:46 am

liukuohao
Posts: 76
Joined: June 17th, 2013, 4:16 am

> **liukuohao wrote:**
> Yes, something like that. Allow what is required to flow out (for example, http, https, dns.....etc....etc)
> So, at the top of firewall rule, you ALLOW traffic http, https, dns.....etc.....etc.
> then at the very last rule, BLOCK all other traffic flowing out from GREEN network to RED.
> If say, a PC in the GREEN network got infected with BOTNET, then it will not able to communicate to its HOST living outside in the RED /WAN network. Just a suggestion only. 😃
>
> Over in pfSense, the people always preach us not to use Default Allow rule.
> Allow what kind of traffic (http, https, dns, ftp...etc) is necessary for your PC GREEN network to work with.
> Block what is not required.

I like take back my I mentioned earlier above.
I tried my method of blocking all unwanted traffic does not seem to work! 😟

Re: I wrote an IPFire Security Hardening guide

by **dnl** » October 24th, 2016, 10:39 am

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

> **liukuohao wrote:**
> I like take back my I mentioned earlier above.
> I tried my method of blocking all unwanted traffic does not seem to work! 😟

Oh, I think it is a good idea.

It takes a lot of effort to do this, but it will improve security.
If you enable logging for the deny rule and then watch the firewall log you can find out which devices are attempting to talk on which ports (or protocols).

The hardest part is going to be software which opens connections on random outward ports.

Re: I wrote an IPFire Security Hardening guide

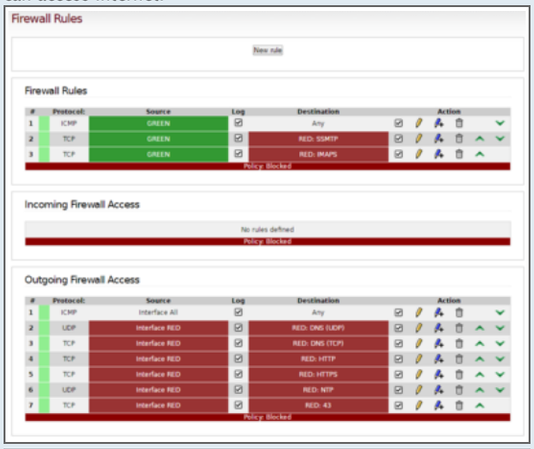
by **mike-us** » November 29th, 2016, 10:26 pm

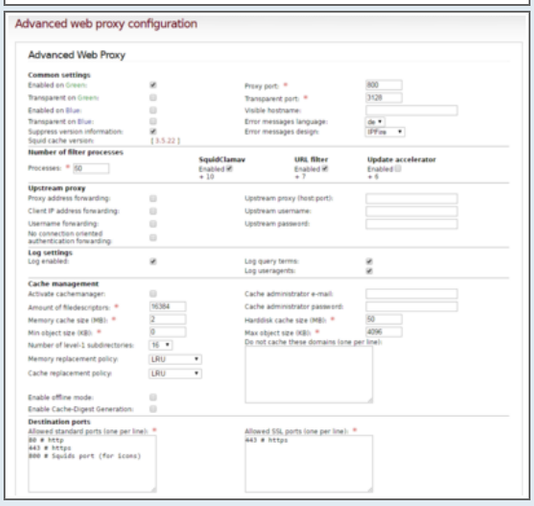
mike-us
Posts: 48
Joined: November 24th, 2016, 2:47 pm

It would be very wise to change Firewall Default Behaviour (FORWARD and OUTGOING) to blocked.
http://wiki.ipfire.org/en/configuration ... ult-policy

This results in no traffic allowed to start with.
After that is set - firewall rules for Basic Services need to be configured - this way you really control what traffic from Firewall to Red and Green to Red is allowed. With Default allowed you have basically no control, DNS, Proxy can just be bypassed by Client PC Settings.

These Rules might be the most useful to start with, because they allow Basic Surfing with activated Proxy and IMAPS and SMTPS for mailing from Green Clients directly. ICMP for Pinging in all directions allowed - just because it makes testing routes easier. NTP from firewall to red so IPFire can get the time - clients can use NTP os IPFire without extra rule. Firewall HTTP / HTTPS so the Proxy and IPFire can access Internet.





If you use Windows Client and want to get Windows Updates this must also run trought Proxy.
=> netsh winhttp set proxy IPFire:Port

Re: I wrote an IPFire Security Hardening guide

by **dnl** » March 5th, 2017, 2:30 am

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

Hey mike-us,

Sorry for the really delayed reply! I've not got much time to tinker these days 😟

That's a great start for a set of instructions for people to configure the outbound firewall.

Would you like to have a go at creating a new wiki page which we could work in to a set of bullet-point instructions for newbies?
I suggest a new page instead of writing it on the Hardening Guide because I think that this will end up being quite long and I'm concerned that the hardening page itself is already too long.

Thanks!

IPFire 2.x (Latest Update) on x86_64 Intel Bay Trail CPU, 4GiB RAM, RED + GREEN + BLUE + ORANGE

Re: I wrote an IPFire Security Hardening guide

by **bamiller1018** » November 27th, 2018, 11:07 pm

bamiller1018
Posts: 2
Joined: November 27th, 2018, 10:55 pm

I would like to start by thanking you for a wonderful guide to hardening IPFire. Your tutorial is concise, accurate, and easy to fallow. On the subject of configuring outgoing firewall rules, a good starting point is to research a subject known as Egress Filtering. I am not certain if I can provide a link to an external site on this forum. However, I can suggest a good starting point.

I suggest dropping outgoing packets from the fallowing protocols to disrupt malware.

MS RPC - TCP & UDP port 135
NetBIOS/IP - TCP & UDP ports 137-139
SMB/IP - TCP port 445
TFTP - UDP port 69
Syslog - UDP port 514
SNMP - UDP ports 161-162
IRC - TCP ports 6660-6669

Cheers

Re: I wrote an IPFire Security Hardening guide

by **dnl** » November 28th, 2018, 9:44 am

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

> **bamiller1018 wrote:** ↑ November 27th, 2018, 11:07 pm
> I would like to start by thanking you for a wonderful guide to hardening IPFire. Your tutorial is concise, accurate, and easy to fallow.

Thanks very much!

> **bamiller1018 wrote:** ↑ November 27th, 2018, 11:07 pm
> On the subject of configuring outgoing firewall rules, a good starting point is to research a subject known as Egress Filtering. I am not certain if I can provide a link to an external site on this forum. However, I can suggest a good starting point.

> I suggest dropping outgoing packets from the fallowing protocols to disrupt malware.
>
> MS RPC - TCP & UDP port 135
> NetBIOS/IP - TCP & UDP ports 137-139
> SMB/IP - TCP port 445
> TFTP - UDP port 69
> Syslog - UDP port 514
> SNMP - UDP ports 161-162
> IRC - TCP ports 6660-6669
>
> Cheers

That's a good starting point!
Most users could also drop SMTP (TCP/25) and IMAP (TCP/143) outbound as in 2018 they should be using SMTP over TLS/SSL or IMAPS. Depending on your needs you could also block, telnet(!), SSH and SFTP oubound too as they're not commonly used in all enviroments (the only exception would be SSH which it might be wise to whitelist for specific sites).

I've not addressed outbound firewall rules yet as I had hoped to use more strict whitelisting of ports/protocols, rather than blacklisting select ones like this. However I like that it is much easier to implement and will be less likely to cause problems.

I'm not sure if you're aware but the new (as of a few years ago) firewall implementation in IPFire now has services defined which can be directly used in rules. So rather than having to enter a protocol and port you can just use a pre-defined service. It makes the main Firewall Rules page much easier to read.

Would you like to edit the wiki page? I'm happy to polish the page later if it helps.

IPFire 2.x (Latest Update) on x86_64 Intel Bay Trail CPU, 4GiB RAM, RED + GREEN + BLUE + ORANGE

Re: I wrote an IPFire Security Hardening guide

by **bamiller1018** » November 28th, 2018, 5:45 pm

bamiller1018

Posts: 2
Joined: November 27th, 2018, 10:55 pm

You are most welcome. Thank you for writing the tutorial. You make a very good point concerning SMTP and IMAP; both are common protocols used by spammers. I also like the idea of creating a restrictive policy around SSH, and whitelisting trusted users.

Two factor verification and the implementation of a hardware random number generator are my next project. Most likely wont be able to edit the wiki for awhile; I would be happy to help out however I can. Thank you for your response, and your input.

Cheers...

Powered by phpBB® Forum Software © phpBB Limited
Privacy | Terms

I wrote an IPFire Security Hardening guide

Re: I wrote an IPFire Security Hardening guide

by **Hellfire** » November 28th, 2018, 6:25 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

> **dnl wrote:** ↑ October 30th, 2015, 9:35 am
> I wrote in the wiki: http://wiki.ipfire.org/en/optimization/ ... _hardening

Is the linked page currently offline of was it deleted? I cannot read this URL ATM.

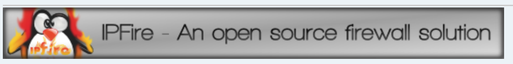
Michael

Re: I wrote an IPFire Security Hardening guide

by **Saiyato** » November 28th, 2018, 9:16 pm

Saiyato
Posts: 36
Joined: October 9th, 2018, 6:55 pm

You can find it here: https://wiki.ipfire.org/optimization/st ... _hardening



Re: I wrote an IPFire Security Hardening guide

by **dnl** » December 2nd, 2018, 5:54 am

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

> **bamiller1018 wrote:** ↑ November 28th, 2018, 5:45 pm
> You are most welcome. Thank you for writing the tutorial. You make a very good point concerning SMTP and IMAP; both are common protocols used by spammers. I also like the idea of creating a restrictive policy around SSH, and whitelisting trusted users.
>
> Two factor verification and the implementation of a hardware random number generator are my next project. Most likely wont be able to edit the wiki for awhile; I would be happy to help out however I can. Thank you for your response, and your input.
>
> Cheers...

Thanks again.

Where are you wanting to implement two factor authentication? With IPFire or in hardening other systems in your network?

IPFire 2.x (Latest Update) on x86_64 Intel Bay Trail CPU, 4GiB RAM, RED + GREEN + BLUE + ORANGE

Re: I wrote an IPFire Security Hardening guide

by **dnl** » December 2nd, 2018, 6:03 am

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

> **Saiyato wrote:** ↑ November 28th, 2018, 9:16 pm
> You can find it here: https://wiki.ipfire.org/optimization/st ... _hardening

Thank you for sending the correct link.

I have now updated the first post.

IPFire 2.x (Latest Update) on x86_64 Intel Bay Trail CPU, 4GiB RAM, RED + GREEN + BLUE + ORANGE