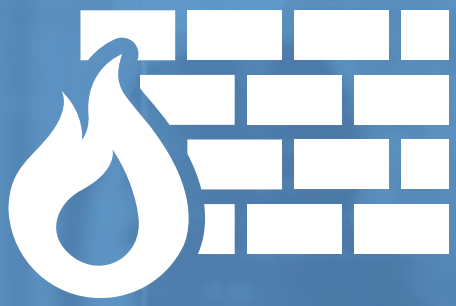


FIREWALL DO'S & DON'TS

31 tips, tricks, and best practices

Ascend TECHNOLOGIES

TABLE OF CONTENTS

CHAPTER ONE

FIREWALL DO'S

22 FIREWALL DO'S

Sizing, web filtering, and alerting...

1. DO: Block by default

Create your policy set so that everything is blocked and you're opening up holes to let things through. It's far easier and less time consuming than doing it the other way around.

2. DO: Get the right-sized appliance

Make sure you understand your network, what you want to do with your firewall, and what kind of load you're going to put on it. Also be sure to consider what features you need now and in the future.

3. DO: Start with web filtering

This is the quickest and easiest to implement, and yet has the most noticeable impact on security right out of the box.

4. DO: Utilize alerting functions

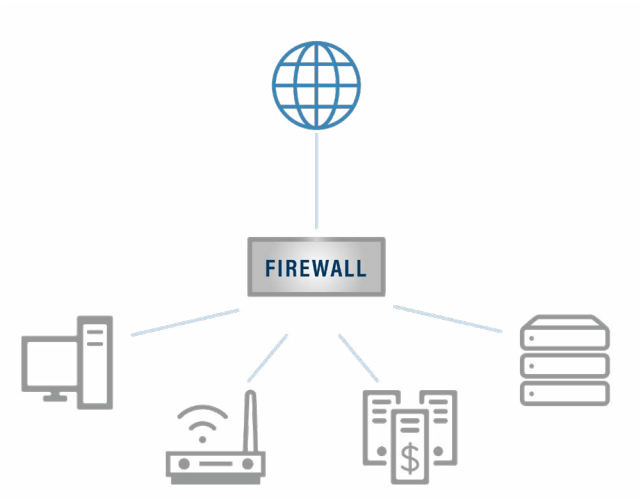
Whether it be from SIEM, a log management tool, or a firewall's built-in alerting mechanism, make use of a technology to immediately alert you of critical events on the firewall. Finding out that the firewall's disk drive is full doesn't do you any good after its been over writing log files for three months.

22 FIREWALL DO'S

Segmentation, logging, and licensing...

5. DO: Divide your network up

Different zones will require different security philosophies. Workstations won't need the same protection that domain controllers would. Always segment your network. If your network is flat, it's easy for malware to spread and a hacker's job just became a whole lot easier.



6. DO: Log everything

Size your firewall so that it can support all of your log activity. As you're implementing new policies and rules, turn on alerting first so you can see what's going across. Be careful of logging too much disk if it's local. You can quickly kill an awesome firewall by pegging it with constant writes.

7. DO: Understand and make use of reporting

Those charts and graphs might seem simple and leave out part of the story but outside of your department they'll provide tangible ROI for both your firewall and your team.

22 FIREWALL DO'S

Firmware, changes, and updates...

8. DO: Keep your licenses current

No brainer, right? Not for some. One of your biggest returns on investment in NGFWs is the vendor's lab, which monitors and studies trends in security and releases frequent updates to best protect your network.

9. DO: Keep your firmware current

Firmware updates can be released to patch vulnerabilities that have been discovered, to release new features, and to improve overall performance of the solution. (Make sure to check out #3 on our "Don'ts" list as well)

10. DO: Track your changes

When a new policy is implemented, make use of the comments field. Note who implemented the policy and when. If you have a change control or ticketing system, leave the reference number in the comments so you can track down why a change was made. You and your coworkers won't be able to remember why you made a rule six months from now.

11. DO: Configure automatic signature updates

Many NGFWs have signature and reputational updates that they receive from the manufacturer. Most of the time these aren't configured to be as often as they should be.

22 FIREWALL DO'S

Passwords, default policies, and rules...

12. DO: Top-down processing on rules

Most firewalls process rules/policies from top to bottom. You want to have your more specific rules near the top for optimized performance.

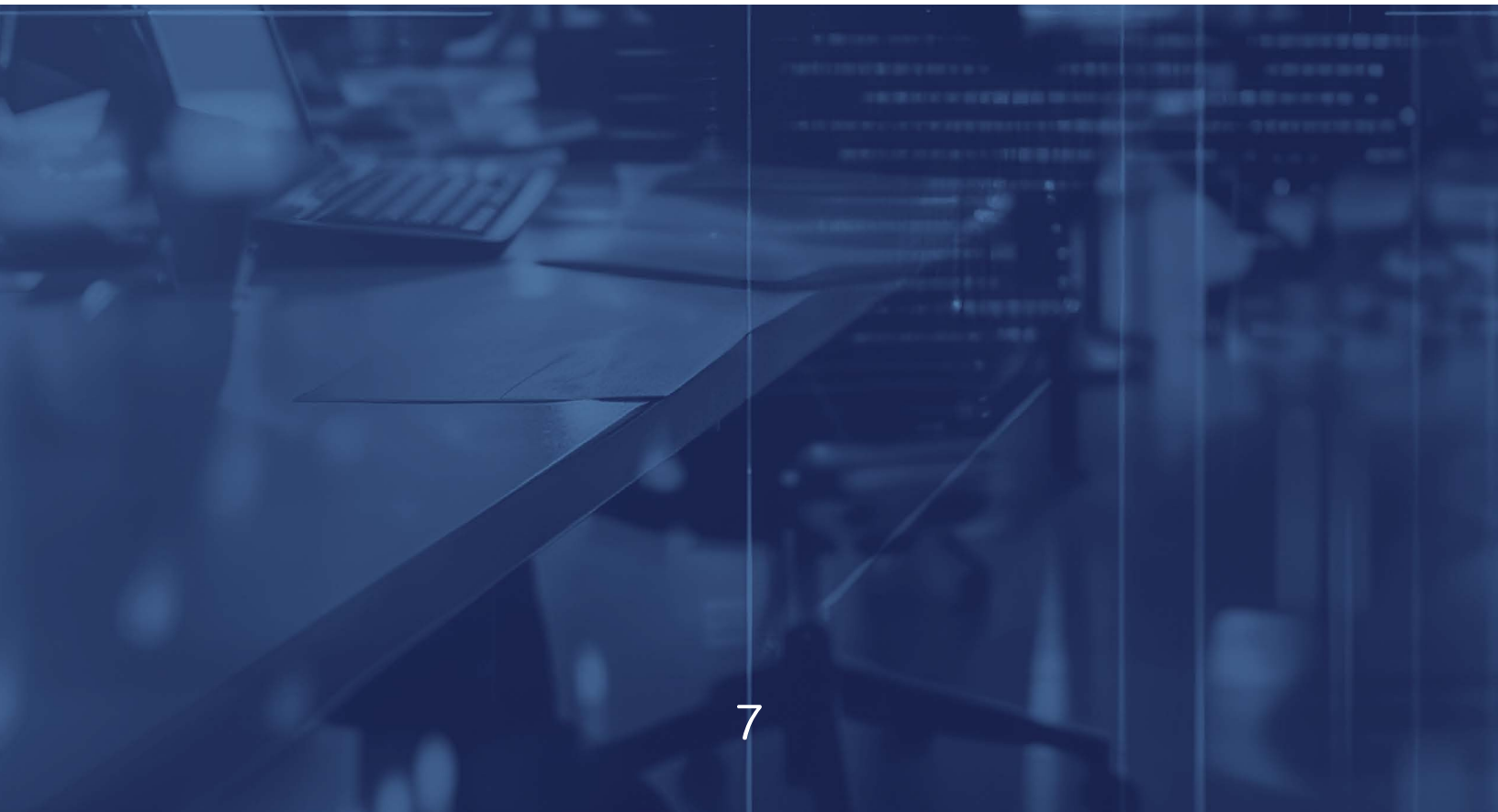
13. DO: Use complex administrator passwords

Think of your firewall as your crown jewels, it needs to be Fort Knox. Many NGFWs have the ability to force strong passwords and restrict logins from certain networks.

14. DO: Be wary of default policies

Manufacturers are incentivized by things like lowering support call volume, increased performance, and customer satisfaction scores. The best security configuration isn't necessarily their starting point.

> **Think of your firewall like your crown jewels. Be sure to require complex administrator passwords to protect your most valuable assets.**



22 FIREWALL DO'S

Backups, configurations, and power supplies...

15. DO: Consider user-based or schedule-based rules

For instance, if you're a bank, do your teller machines need to access the internet outside of business hours? This allows you to look at any traffic generated after hours with a skeptical eye and prevent exfiltration when you are not there.

16. DO: Configure Network Time Protocol (NTP)

Make sure the NTP is configured so that your firewall clock is always accurate for log review and investigations.

17. DO: Have high availability and/or dual power supplies

Hardware fails. We see a lot of banks, hospitals and government entities that opt for a single firewall. Saving those few thousand dollars up front is not worth your entire organization being down for 1-3 days in most cases.

18. DO: Configure automatic backups

Too many people forget their firewalls in their backup strategy. Firewall changes happen, so configuring automated backups, preferably kept off-site, is the goal.

22 FIREWALL DO'S

DNS servers, applications, and visibility policies...

19. DO: Block access to Domain Name System (DNS) servers

Block access to DNS servers that aren't your preferred or provided hosts. Why make it easy on malware to use whatever DNS servers they want in the world? You should also pay attention to DNS servers that aren't yours, blocked or not.

20. DO: Visibility vs. block approach when testing policies

NGFWs have the ability to identify applications moving through your network. You don't have to block applications just to have visibility and know what's going on.

21. DO: Block unauthorized applications

Block access to applications like proxies or remote access apps that aren't approved. You should also pay attention to employees that are trying to use them as they may be trying to circumvent your security controls.

22. DO: Implement anomaly-based rules & alerts

Or as we like to call them, 'Snowden Rules'. If someone is uploading or downloading gigabytes of data and never has before, it might be worth an email. Or if a marketing person's workstation is utilizing a Secure Shell to host on the internet, you should probably investigate.

CHAPTER TWO

FIREWALL DONT'S

9 FIREWALL DON'TS

Onboarding, monitoring, and internet rules...

1. DON'T: Use internet rules with 'ALL' in them

Blocking inbound traffic while creating no rules to cover your users' outbound traffic leaves you wide open to a legions worth of potential threats.

2. DON'T: Do it all at once

Day one is not the time to turn on every function that the firewall has. Prioritize based on your risk tolerance and the nature of your business.

3. DON'T: Keep your firmware TOO current

Unless a patch is released to address a critical vulnerability, it's best to watch release notes and monitor web locations discussing issues other customers are experiencing. Give new firmware some time in the wild before updating. Let other people be the guinea pigs.

> **Don’t rush into the newest updates. Give new firmware some time in the wild before updating. Let other people be the guinea pigs.**

9 FIREWALL DON'TS

IPS signatures, encrypted traffic, and attention...

4. DON'T: Ignore your NGFW

Like anything else in life, you get out of your NGFW what you put in to it. Spend some time learning what it can do and how it can best make an impact in your organization. Be sure to monitor and review events, performance, and user activity!

5. DON'T: Perform unnecessary security filtering

Avoid unnecessary filtering on traffic flows. If you trust traffic between two zones, don't turn on full inspection or all security features.

6. DON'T: Look for unnecessary IPS signatures

Don't look for IPS signatures in operating systems you aren't protecting. If the only servers you are protecting are Windows, don't enable Linux IPS signatures. There isn't any value and you will be make your firewall check packets against more signatures.

7. DON'T: Be blind to encrypted traffic

Hackers and most of the internet use SSL inspection. Don't be blind to to traffic that is encrypted if your business (and lawyers) allow you to do so.

9 FIREWALL DON'TS

Changes and simplicity

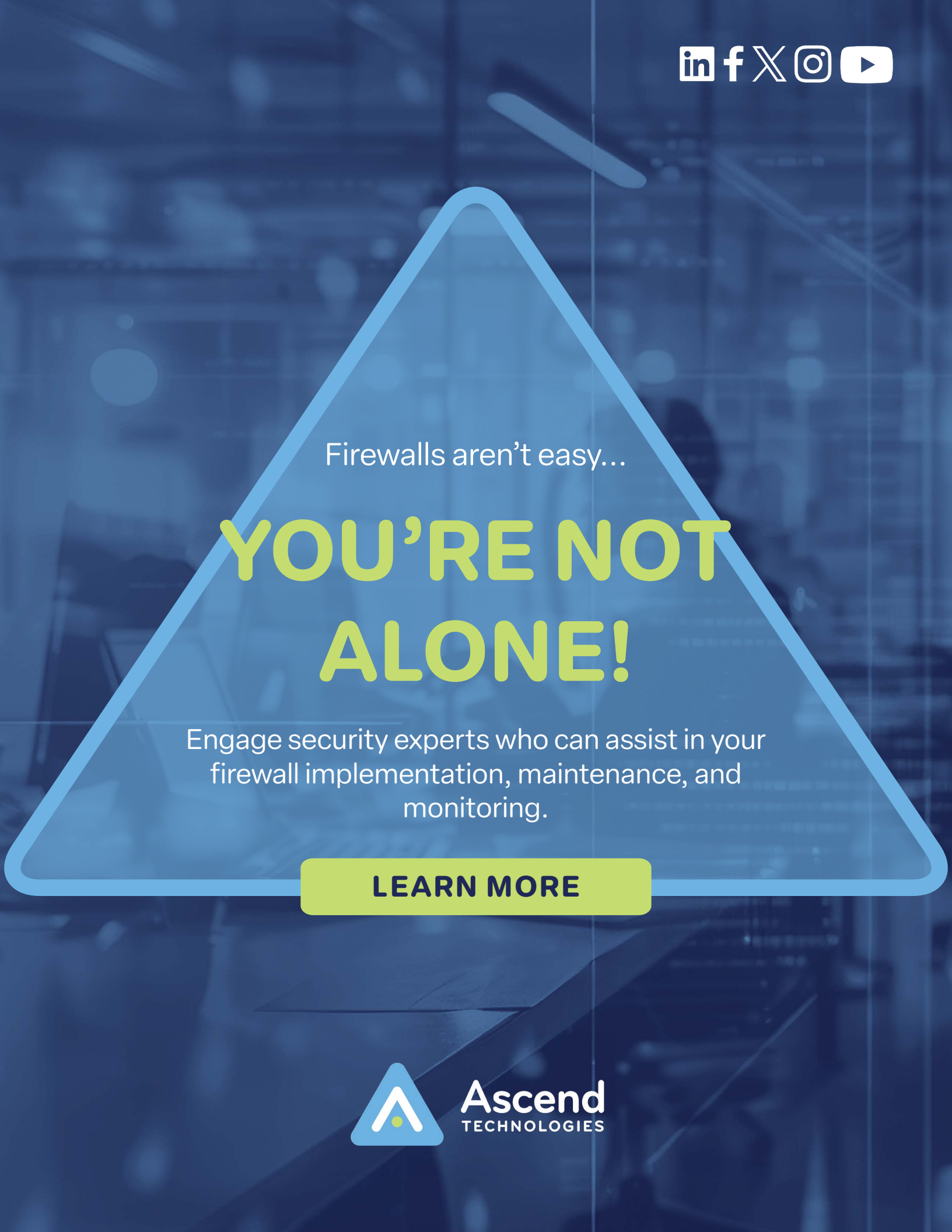
8. DON'T: Make random changes

Just because you can configure and change things, doesn't mean you should. Unless you're confident in what you're changing and why, it's probably best to leave it alone. The manufacturer is usually good at optimizing their own products.

9. DON'T: Overthink it

Don't get too granular. While it can be good, it can also be a performance killer. Fewer rules and objects can be a good thing where possible.

Looking for more information about firewall configuration and management? Check out our firewall management offerings.


Firewalls aren't easy...
YOU'RE NOT ALONE!
Engage security experts who can assist in your firewall implementation, maintenance, and monitoring.
LEARN MORE
Ascend
TECHNOLOGIES