Cyber security

Firewall 101: **What every business should know**

Sussex Tech Support

You can’t see it.

You can’t touch it.

But right now, it’s quietly standing between your business and thousands of online threats.

Every single email you send, website you visit, or file you download passes through it.

And if it wasn’t there, your business would be wide open to attack.

That invisible protector is your firewall.

A firewall is a bit like the security guard at the entrance to your office building.

It checks everyone coming in and out, deciding who’s allowed through and who should be stopped at the door.

When it recognises something safe, it lets it in. When it spots something suspicious, it blocks it before it causes harm.

You might not notice it working, but every second it’s filtering millions of digital “visitors” keeping out cyber criminals, viruses, and other nasty surprises.

But even the best firewall can’t protect you from everything.

Your team must still move around the online world safely. And that’s where web filtering comes in.

Think of web filtering as your business’s “satnav” for the internet.

It helps guide your people away from dangerous or inappropriate sites and towards safe, trusted destinations.

It’s the extra layer that keeps both your data and your reputation intact.

Together, your firewall and web filter act like a security team that never sleeps.

One stands guard at the gate. The other keeps an eye on where everyone goes once they’re inside.

Without them, your business would be an open target.

With them, you’re protected. Often without even realising it.

So, what is a firewall?

Imagine your business is a building.

Inside are your people, your equipment, your files. Everything that keeps things running.

Now picture the internet as the world outside that building. It's huge, busy, full of opportunity… and full of risk.

You want customers and partners to visit. You want your team to send and receive information. But you don't want strangers wandering in off the street.

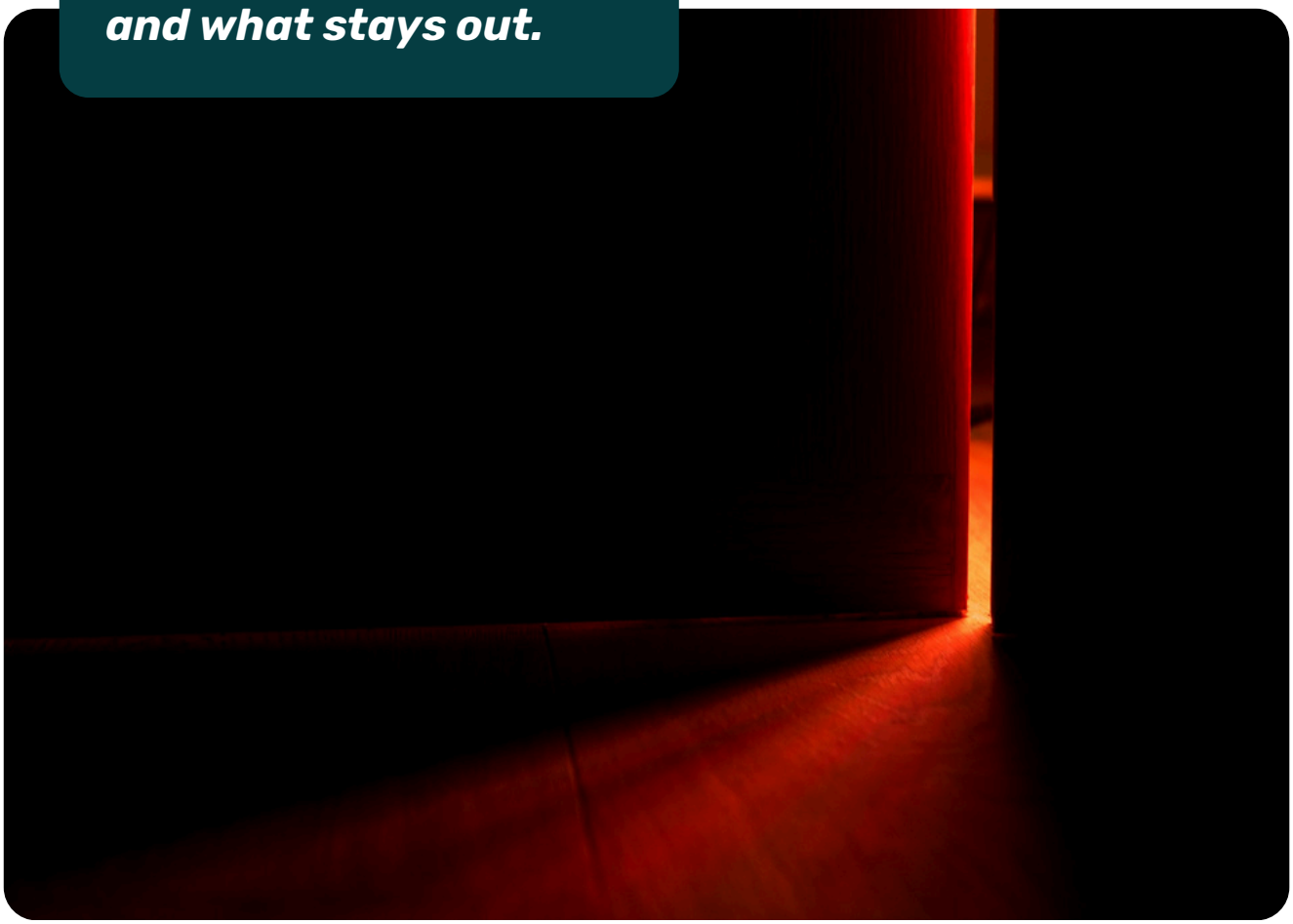
That's where your firewall comes in.

Every time data tries to move between your network and the internet, the firewall checks it.

If it's safe, like a trusted website or a regular email, it opens the gate and lets it through.

If it's suspicious, like a hacker's attempt to break in or a malicious file, it keeps the gate firmly shut.

It decides what gets in and what stays out.



How it works

The firewall watches all incoming and outgoing traffic on your network.

It compares each bit of data against a list of rules (known as policies) to decide what's allowed.

These rules might say things like:

- "Let staff access this trusted website."
- "Block any file that looks like malware."
- "Don't allow unknown connections from the outside."

It's security for your business data, scanning what comes in, what goes out, and making sure no one sneaks through with something dangerous.

Do you already have a firewall?

Almost certainly, yes.

If your business connects to the internet through a router (the small box that gives you Wi-Fi), it likely has a basic firewall built in.

But those built-in firewalls are often designed for home use, not for protecting a busy workplace. They might block the obvious threats, but they don't always keep up with the more sophisticated attacks that target businesses.

That's why many companies use dedicated firewalls, often managed by their IT support partner, that provide stronger protection, regular updates, and 24/7 monitoring.

Why firewalls matter more than you think

You might not notice your firewall doing its job, but it's working constantly in the background.

Every second, it's scanning data, applying rules, and quietly blocking countless attempts to get in.

Without it, your network would be open to:

- Hackers trying to steal your data
- Malware (harmful software) infecting your systems
- Ransomware attacks that lock your files until you pay a fee
- Unauthorised access from devices that shouldn't be there

Your firewall is your first line of defence, but it can't do the job alone. It needs the right setup, regular updates, and a few supporting tools to cover every angle.

How firewalls protect your business

Your firewall is the unsung hero of your IT setup.

And it has one goal: To stop trouble before it starts.

Every time a computer or phone in your business connects to the internet, data starts flowing in both directions. Tiny packets of information being sent and received.

Your firewall checks each of those packets to make sure they belong.

It knows what safe traffic looks like (for example, a staff member opening your cloud accounting system), and it knows what suspicious traffic looks like (a strange connection from an unknown location at 3am.).

If something doesn't fit the pattern, the firewall blocks it. Instantly.

This is what keeps out most of the automated hacking attempts that happen all day, every day. You'll never even know they were there, because your firewall quietly dealt with them.

Protecting against common threats

Here are a few of the most common dangers your firewall defends against:

Hackers - People trying to break into your systems, usually to steal data or cause disruption. Your firewall stops their attempts to connect to your network.

Malware - Short for "malicious software," this covers things like viruses, spyware and ransomware. Your firewall helps stop these from entering in the first place.

Phishing attacks - These are emails or websites pretending to be legitimate, trying to trick you into giving away passwords or payment details. A good firewall can block access to known phishing sites.

Botnets -These are groups of infected computers controlled by hackers. A firewall can prevent your devices from accidentally joining one or communicating with them.

Modern firewalls are clever. They don't rely on a fixed list of "good" and "bad" connections. They use smart analysis, sometimes called stateful inspection, to look at what's happening in real time.

That means if someone in your business downloads a file that suddenly starts behaving oddly (for example, trying to talk to a server in another country), the firewall notices and shuts it down.

A firewall doesn't work in isolation. It's part of your wider security setup.

It works with tools like:

Security software, which scans files on individual computers for infection.

Email filters, which catch spam and phishing attempts before they reach your inbox.

Multi-factor authentication (MFA), which makes sure only the right people can log in.

Your firewall is the gatekeeper, but once you're inside, the others keep things tidy, safe, and monitored.

Without a properly configured firewall, even a small slip can have big consequences.

All it takes is one exposed connection or one staff member clicking a bad link, and an attacker can slip through.

Once inside, they can move quickly, copying files, installing ransomware, or stealing login details.

And what's worse, is many businesses don't realise they've been breached until days or even weeks later.

A good firewall reduces that risk dramatically. It watches for unusual activity and raises alerts before real damage is done.

The different types of firewalls

Not all firewalls are created equal.

Some are basic. They block the obvious threats and that's about it.

Others are much smarter. They understand what's happening on your network in real time and can adapt to stop new kinds of attacks.

The difference matters, because cyber criminals never stop inventing new tricks.

Packet filtering firewalls

This is the oldest and simplest type of firewall.

A packet filtering firewall examines small chunks of data (called packets) that try to pass through your network.

It looks at basic details, like:

- Where the data came from
- Where it's going
- What type of connection it's using

If it matches the rules you've set, it's allowed in. If not, it's blocked.

It's quick and efficient, but not very clever. It can't tell if something looks suspicious once it's already inside, or if a "trusted" connection suddenly starts doing something unusual.

Stateful inspection firewalls

A stateful inspection firewall goes a step further.

Instead of checking each packet on its own, it watches the whole conversation between devices.

This kind of firewall understands what a normal connection looks like and can spot when something seems out of place.

It's been the standard for business use for many years and still offers solid protection today.

Next-generation firewalls (NGFW)

These are the high-tech bodyguards of the firewall world.

A next-generation firewall does everything the older types do, but it also includes extra layers of protection built for today's threats.

Here's what sets them apart:

Deep inspection: They look inside the data itself, not just the envelope it arrived in.

Intrusion prevention: They can automatically block suspicious behaviour before damage occurs.

Application awareness: They recognise specific programs and can control which ones are allowed to communicate over the network.

Threat intelligence updates: They regularly receive new information about the latest cyber attacks, keeping their defences current.

In short, they're proactive rather than reactive. They don't sit back and wait for something to go wrong.

Cloud firewalls

As more people work remotely, many businesses are moving parts of their security to the cloud.

A cloud-based firewall performs the same job, but it's hosted on the internet rather than on a physical box in your office.

This means protection travels with your people, whether they're in the office, at home, or connecting from a coffee shop.

It's especially useful if your business has multiple sites or remote workers who need the same level of safety wherever they are.

Managed firewalls

A firewall is only as strong as its setup.

The rules, updates, and ongoing monitoring all matter.

That's why many small and medium sized businesses use managed firewalls, where an IT support partner looks after everything for them.

That includes:

- Installing and configuring the right firewall for your needs
- Keeping it updated as threats evolve
- Watching for suspicious activity 24/7
- Adjusting rules as your business changes

It's like having a dedicated security team without having to employ one in-house.

Each of these firewalls plays a role in keeping businesses safe, but together they tell one clear story. Firewall technology has grown smarter, faster, and far more capable than ever before.

And while the differences in names might sound technical, the goal hasn't changed:
To stop anything dangerous before it reaches you.

Web filtering is just as important

Even with the best firewall in place, your business can still run into trouble.

That's because not every threat forces its way in. Sometimes your team accidentally invites it in.

A click on the wrong link. A quick visit to a risky website. A download that looks innocent but isn't.

It only takes one moment of distraction for a cyber threat to slip through the cracks.

What web filtering does

A web filter controls which websites your team can visit when connected to your business network.

It works like a safety net between your people and the wider internet, blocking access to dangerous or inappropriate sites before they load.

Web filters can:

- Stop access to websites known for spreading malware (harmful software)
- Prevent phishing pages that try to trick people into entering passwords or financial details
- Block unsuitable or time-wasting content such as adult sites, gambling, or social media (if you choose)
- Reduce the risk of someone downloading malicious files by mistake

Think of it as a guide for safe browsing. It doesn't stop people from working. It helps them avoid the digital equivalent of a dark alley.

There are two big reasons every business needs web filtering:

Security: Even the most cautious employees can be fooled by a convincing link or fake login page.

A web filter blocks these pages before anyone has a chance to fall for them, stopping the problem at the source.

Productivity: Let's be honest, the internet is full of distractions.

A well-set-up web filter helps your team stay focused on work-related sites, not personal browsing or videos.

A web filter is not for policing your staff. It's there to keep everyone safe and on track.

How it works behind the scenes

When someone types a web address or clicks a link, the web filter checks it against a massive database of known websites.

That database groups sites into categories, such as “business”, “shopping”, “social media”, or “malware”.

Based on your company’s policy, the filter decides what’s allowed and what’s not.

For example:

- A visit to your bank’s website? **Allowed.**
- A site hosting pirated movies or suspicious downloads? **Blocked.**

Many web filters also analyse new or unknown sites in real time, checking for suspicious behaviour or hidden code.

If a site looks risky, it’s stopped automatically, often within milliseconds.

Web filtering can be tailored to suit your business, your people, and your values.

You can:

- Allow access to social media for your marketing team, but not for everyone
- Permit streaming sites for training videos, but block them elsewhere
- Give management a different level of access than general staff

The risks of not having web filtering

Here’s what can go wrong when you don’t have web filtering:

- A single click on a bad link installs malware across your network
- Employees accidentally visit fake websites that steal login details
- Productivity drops as people drift into non-work sites during the day

And worst of all, these problems often start small but grow fast, costing time, money, and reputation to fix.

If your firewall is the security guard standing at the door, your web filter is the guide helping everyone inside make smart choices.

They work best together:

- The firewall blocks attacks trying to break in
- The web filter prevents your people from walking into danger zones online

Together, they protect your business from both sides, keeping out the threats you can’t control and limiting the risks you can.

Common firewall mistakes

Most businesses do have a firewall.

The problem is many of them aren't using it properly.

Firewalls don't just work by being plugged in. They rely on good setup, maintenance, and monitoring to keep doing their job.

And that's where many small businesses slip up.

Using the default settings

When a new firewall is installed, it often comes with "default" or factory settings.

These are designed to get things running quickly. But they're not tailored to your business.

Default settings can leave unnecessary ports open or fail to block certain risky types of traffic.

A properly configured firewall should be customised to your specific needs. The size of your business, the types of data you handle, and the tools your team uses.

Without that, you're only getting half the protection you think you have.

Setting and forgetting

This is one of the biggest mistakes of all.

A firewall isn't something you install once and walk away from.

Cyber threats change constantly. What protected you two years ago might not protect you today.

Firewalls need regular updates, just like your phone or computer. These updates fix vulnerabilities and teach the system how to recognise new attacks.

If your firewall hasn't been updated or reviewed in a while, it may be quietly falling behind.

Relying on a home-grade router

Many businesses start out using the router that came from their internet provider. The same type you might use at home.

The issue?

Home routers have very basic firewalls. They're fine for family browsing, but not for protecting business data, customer records, or multiple employees online at once.

They often lack advanced features like:

- Intrusion prevention
- Real-time threat monitoring
- Detailed reporting and alerts

A business needs business-grade protection. It's that simple.

No one is watching the alerts

Your firewall is constantly collecting information. Logging every blocked attempt and sending out alerts if it spots something strange.

But if no one's looking at those alerts, you might not notice a problem until it's too late.

This is why so many companies now use managed firewalls. An IT support provider monitors things on your behalf, checks alerts in real time, and deals with issues before they become disasters.

If your business doesn't have that kind of support, it's worth asking: *Who's keeping an eye on your defences right now?*

Trying to do too much with one device

Some businesses rely on a single piece of equipment to handle everything. Firewall, Wi-Fi, web filtering, and more.

That's convenient, but it can also overload the system and slow down your network.

When too many jobs are packed into one box, performance suffers. And sometimes, so does protection.

A better setup might separate some of those roles or use a dedicated next-generation firewall designed to handle them efficiently.

Ignoring remote workers

Lots of employees work from home or on the go.

If their devices aren't protected by your main firewall, or if they connect through unsecured Wi-Fi, your network could still be at risk.

The best approach is to extend protection beyond the office using a cloud-based firewall, which filters traffic wherever users connect from.

That way, your security perimeter moves with your people.

No regular review or testing

Even if your firewall was set up perfectly, things change.

You add new software, hire new staff, expand to a second site, and every change affects your network traffic.

Regular reviews help ensure your firewall's rules still make sense.

A quick check every few months can catch gaps or outdated rules long before they turn into real problems.

None of these mistakes are unusual. In fact, most businesses have made one or two at some point.

The important thing is knowing where the weak spots are and taking simple steps to fix them.

A well-configured firewall is part of your business's safety plan. And when it's set up right, updated regularly, and monitored properly, it quietly protects everything you've worked so hard to build.

How to choose the right firewall for your business

Choosing a firewall means finding the right level of protection for your business. One that fits how you work, how your team connects, and what kind of data you need to protect.

There's no single "best" firewall for everyone.

The perfect setup for a five-person accountancy firm will look very different from what a manufacturing company with two sites needs.

But the good news is that you don't need to be a tech expert to make the right choice. You just need to understand the basics.

1

Start with how your business operates

Before thinking about brands or features, look at how your business actually uses technology.

Ask yourself:

How many people are connecting to your network?

- Where do they work? All in one office, or in multiple locations?
- Do you have remote staff working from home or on the road?
- What kind of data do you handle? Financial details, personal information, or internal systems?
- Are there industry rules (like GDPR or data protection standards) you need to meet?

The answers help determine what kind of firewall setup you'll need. Whether a simple on-site device will do, or if you'll benefit from a managed or cloud-based solution.

2

Hardware vs. software vs. cloud

Firewalls come in three main forms, and each has its strengths.

Hardware firewalls are physical devices that sit between your network and your internet connection. They're powerful, reliable, and ideal for businesses with a central office or server.

Software firewalls run on individual computers or servers. They're useful for protecting specific devices, especially laptops used by remote workers.

Cloud firewalls live online, protecting data wherever it travels. These are great for modern businesses with remote teams, multiple offices, or a mix of in-office and mobile devices.

Many companies now use a combination. A hardware firewall in the office and cloud protection for staff working remotely.

3

Features that matter most

There's no shortage of options when it comes to firewall features, but not all are essential for smaller businesses.

Here are the ones that usually make the biggest difference:

Next-generation protection: Includes intrusion prevention, deep inspection of data, and built-in antivirus scanning.

Automatic updates: Keeps your firewall aware of new threats without needing manual input.

Web filtering: Stops users from visiting harmful or time-wasting sites.

Monitoring and reporting: Gives you visibility into what's happening on your network and any threats being blocked.

If you're unsure which features you need, an IT support partner (like us) can help you strike the right balance between protection, performance, and cost.

4

Think about management and maintenance

Many businesses underestimate how much attention a firewall needs once it's installed. That's why managed firewalls have become so popular.

With a managed service, your IT support partner handles:

- Configuration and setup
- Continuous monitoring
- Regular updates and patches
- Real-time alerts and reporting

You get enterprise-level security without having to think about it day to day.

5

The cost question

Firewalls range from affordable to very expensive. But the price difference usually reflects the level of protection and support you get.

For most small and medium sized businesses, the right question isn't "What's the cheapest?" but "What's the best protection we can get for our budget?"

A few hundred a year on the right firewall can prevent losses of thousands, or even tens of thousands, in the event of a data breach or ransomware attack.

It's an investment in peace of mind.

6

Don’t go it alone

The smartest move you can make when choosing a firewall is to involve an expert.

Tech professionals understand how to match security tools to business needs. We assess your setup, explain your options clearly, and make sure everything is properly configured.

The right firewall is a vital part of your business’s security foundation. It’s important to get it right.

If your business needs expert advice, we’d love to help.

Get in touch.

CALL: 01444 223850
EMAIL: contact@sussex.tech
WEBSITE: www.sussex.tech

Sussex Tech Support
SECURITY TRUST SERVICE