QOS MSP
Managed Services

NETWORK SECURITY STACK PLANNING:

A BUYER'S GUIDE FOR BUSINESS LEADERS

The five layers of a business security stack, the sizing questions to answer before you buy, and the one-time-versus-recurring cost model — so you can read a security quote line by line.

☎ +1 (877) 800-7672

www.qosmsp.com

Network Security Stack Planning: A Buyer's Guide for Business Leaders

Somebody sent you a quote for a firewall. It has a model number, a three-year subscription line, an installation line, and a total. You have no way to tell whether it is the right size, what the subscription actually renews, or what it will cost to keep running in year two.

That is the problem this guide solves. It is not a product recommendation and it is not a sales sheet. It is the set of questions we ask before we scope a security stack — written down so you can ask them of us, or of whoever else is quoting you.

1. Why This Guide Exists

Most small and mid-sized businesses never chose their network security. It arrived with the internet circuit. The ISP left a router with firewall features switched on at defaults, someone opened a few ports over the years, and that has been the security layer ever since.

An inherited stack is not incompetence — it is just what happens when nobody was ever asked to design one. The trouble is that it fails quietly. There is no alarm for "the guest Wi-Fi can reach the accounting server" or "that port forward belongs to a vendor we stopped using in 2021."

Who this is for:

- Business leaders holding a security quote they cannot evaluate
- Companies whose firewall is out of vendor support or near it
- Multi-site or hybrid operations that grew past their original network
- Anyone who inherited a network and wants to know what they inherited

What this guide is not:

- **Not a DIY checklist.** If you want the controls you can implement yourself, read our small-business cybersecurity checklist instead — that is the do-it-yourself companion to this document.
- **Not a compliance guide.** Frameworks and audits are a separate discipline with separate requirements. Nothing here is written to satisfy an auditor.
- **Not a monitoring service pitch.** This is about designing and installing a stack — the build, not the ongoing watch.

The Goal:

You finish this guide able to scope, size, and budget a security stack build — and able to tell a good quote from a lazy one.

2. The Five Layers, and What Each Actually Does

“Network security” is not one product. It is five layers that get designed together and installed as one build. Here is what each one is for, and the honest signal that you need it.

Layer 1 — The Firewall

The firewall decides what traffic is allowed to cross the boundary between your network and the internet, based on a rule base someone wrote on purpose. A business firewall also inspects the content of allowed traffic, which is what the vendor subscription pays for. An ISP router with a checkbox labeled “firewall” is not this.

You need this when: your edge device came from your ISP, is out of vendor support, or nobody can produce a list of its rules.

Layer 2 — VPN and Secure Remote Access

A VPN gives remote staff an encrypted tunnel into business systems, so those systems never have to be exposed to the open internet. Site-to-site VPN does the same between offices. The alternative — forwarding a port to an internal server — publishes that server to every scanner on the internet.

You need this when: anyone works from outside the building, or you have more than one location that shares systems.

Layer 3 — Intrusion Detection and Prevention (IDS/IPS)

IDS/IPS inspects the traffic the firewall allows through, matching it against known attack patterns, and blocks or flags what looks wrong. The firewall is the door; IDS/IPS watches what walks through it. Its signature feed is a subscription because attacks change weekly.

You need this when: you have anything worth reaching on the inside — which, at this point, is every business.

Layer 4 — Network Segmentation

Segmentation splits one flat network into VLANs with rules about what may talk to what: guest Wi-Fi here, voice there, cameras and point-of-sale on their own, business systems isolated from all of it. It is the layer that decides how far a breach travels. On a flat network, everything reachable by the intruder is everything you own.

You need this when: guest, voice, camera, or POS traffic shares a network with the systems that run your business.

Layer 5 — Monitoring Setup

Logging, alerting, and monitoring agents make the stack watchable: the devices report what they see to somewhere a human will actually look. Note the word *setup*. This layer is the plumbing that makes monitoring possible — who watches it, and when, is the subject of section 6.

You need this when: you could not answer “when did that firewall last block something?” without guessing.

The Rule:

The layers are cumulative, not optional courses on a menu. A firewall without segmentation still lets a breach roam; segmentation without a VPN still leaves open ports; any of it without monitoring setup means nobody finds out.

3. Sizing Questions to Answer Before You Buy

A firewall quote without these answers is a guess with a price on it. Get them written down before anyone quotes you — including us.

Answer These:

- **How many users?** Not headcount — concurrent devices, including phones and tablets.
- **How many sites?** Each one needs an edge device and a route to the others.
- **What is your WAN bandwidth?** Today, and what you have already ordered for next year.
- **How many people work remotely?** Concurrent VPN users, at peak, not on average.
- **What else is on the network?** Guest Wi-Fi, VoIP phones, cameras, point-of-sale, building systems, machinery — each is a segmentation decision.
- **What throughput do you need with inspection turned on?** This is the question that separates real quotes from bad ones (see below).
- **Do you need high availability?** A second firewall that takes over automatically roughly doubles hardware cost. Whether that is worth it depends on what an hour of downtime costs you.

The Red Flag:

Firewall datasheets advertise a headline throughput number measured with inspection off. With threat inspection actually enabled — the reason you are buying the thing — real throughput is a fraction of that figure. A quote sized against the headline number will hit a wall the day the security features are switched on. Ask which number the sizing used.

The Goal:

Every line on your quote traces back to one of these answers.

4. One-Time vs. Recurring: The Cost Model

This is the section people skip and then regret. A security stack has four cost lines, and they do not behave the same way. Two are one-time, two renew forever.

What you're buying	What it covers	Price
Security stack design and installation	Assessment, engineering, firewall/VPN/IDS/segmentation configuration, installation, and documentation	Quoted per engagement
Managed network device	Ongoing management of one firewall, switch, or access point	$25/month per device — management only
Hardware	Firewall, switch, and access point purchase	Billed separately
Vendor security subscriptions	Firewall security services, access point licensing, IDS/IPS signature feeds	Billed separately

The $25 per-device rate covers management only. Hardware and vendor security subscriptions — firewall security services, access point licensing, IDS/IPS signature feeds — are billed separately.

Why the Subscriptions Renew:

The subscription lines are the ones that surprise people in year two. A firewall's threat inspection, its IDS/IPS signature feed, and its content filtering are not features you buy once — they are feeds that only work if they stay current, because the attacks they match against are new every week. When the subscription lapses, the hardware keeps running and quietly stops inspecting. Budget them as an operating cost from day one, not as an optional add-on you can drop later.

Why the Build Is Quoted, Not Listed:

We do not publish a flat build price because a 15-person single office and a four-site operation with 40 remote staff are not the same project, and pretending otherwise means one of the two gets a wrong number. The build is quoted after an assessment, against the answers from section 3.

The Rule:

Ask any vendor to break a quote into these four lines. If they cannot, or if hardware and subscriptions are bundled into one number you cannot decompose, you cannot compare their quote to anyone else's — and you will not see year two coming.

5. What “Done” Looks Like

A build is finished when you can hold the evidence, not when the appliance blinks. Every one of these is a deliverable you should expect to receive — and should ask for by name if the quote does not mention them.

Require All Five:

- **A firewall rule base document** — every rule, what it is for, and who asked for it. This is the artifact that lets the next engineer — ours or yours — touch the firewall without guessing.
- **A network diagram** — the segments, what lives on each, and what is permitted to cross between them.
- **VPN client configuration** — documented setup, tested from outside your network, with a written procedure for adding the next user.
- **An IDS/IPS baseline** — tuned to your traffic, so alerts mean something. An untuned sensor produces noise, and noise gets ignored.
- **Monitoring in place** — logging and alerting live, pointed somewhere a person will see them, on the day the stack goes live.

The Red Flag:

“It’s installed” without documentation is not done. It is a black box you now depend on, and the only person who understands it does not work for you.

6. What Happens After Install

Here is the part most security quotes leave out: a stack without an owner decays. Firewall rules accumulate as people ask for exceptions. Subscriptions lapse. Firmware falls behind. VPN accounts for departed employees stay enabled. Nothing announces any of it.

The build and the run are two different jobs. Designing and installing the stack is project work with an end date. Keeping it current — threat monitoring, patching, MFA enforcement, incident response — is an ongoing role called security administration. Someone has to hold it: a person you hire, or a provider you retain.

QOS MSP does both, which is why we say this plainly rather than selling you the build and walking away. Our managed network device rate is what covers the device side of that ongoing work; the broader security role is priced per user. What matters is that you decide who owns it *before* the install, not eighteen months later when someone asks why the subscription expired.

The Rule:

Do not buy a stack you have no plan to maintain. An unmaintained security stack is a security stack that was accurate on installation day.

7. Start Here: The Decision Tree

Two honest paths. Pick by answering one question: **can you name what is wrong?**

If yes — go straight to a build.

You can point at it: the firewall is out of vendor support, remote access runs through open ports, the network is flat, a site needs a VPN. The problem is defined, so the build can be scoped against it. Get the section 3 answers together and ask for a quote broken into the four lines from section 4.

If no — get a cyber risk assessment first.

You know something feels wrong but cannot say what. Do not buy hardware yet. A stack build is the wrong first purchase when nobody has defined the problem — you would be spending on equipment to solve something nobody has named. A cyber risk assessment finds what is actually exposed and ranks it, and then the build gets designed against real findings instead of assumptions. Sometimes the assessment finds the firewall was never the issue.

Either way — the checklist is free.

Our small-business cybersecurity checklist covers the controls you can verify yourself, at no cost, before either conversation starts. It is the DIY companion to this guide.

The Bottom Line:

We would rather scope an assessment than sell you a firewall you may not need. A stack built against a guess is an expensive guess.

8. About QOS MSP

QOS Consulting was founded in 2007 and has been engineering business networks ever since — nearly two decades. QOS MSP is its managed-services arm: the team that designs, installs, documents, and runs those networks for small and mid-sized businesses across Indianapolis and Indiana.

Our leadership carries more than 30 years of IT experience, and we have supported over 75,000 users across client environments. We are vendor-neutral on firewall and IDS selection — we size to your traffic, not to whichever line card pays best. And we are not a 24/7 security operations center; we are the team that builds the stack correctly and runs it honestly. When a business genuinely needs round-the-clock threat hunting, we say so.

Talk to an Engineer:

- **Phone:** +1 (877) 800-7672
- **Web:** www.qosmsp.com
- **Schedule a free consultation:** calendly.com/qosconsulting/new-customer — no cost, no obligation

The Final Word

The businesses that get security right are not the ones that spent the most. They are the ones that knew what they were buying, sized it against their own traffic, and decided who owned it before the box arrived.

An inherited stack is not a decision. It is the absence of one. The whole point of this guide is to replace it with a decision you made on purpose — and can explain, line by line, to anyone who asks.

Next Step:

Find your firewall. Look up its model number and check whether it is still under vendor support and whether its security subscription is current. That single answer — which takes about ten minutes — tells you whether you are planning a build or already overdue for one.