



AMBIO IT SOLUTIONS

NETWORK RISK ASSESSMENT · SAMPLE REPORT

Network Health Report & Remediation Roadmap

Northgate Family Health (fictional customer)

Single site — 2-story medical office, Sacramento, CA

Assessment window: 2026-09-14 — 2026-09-25

Tier: **Edge Assessment — Small Business**

01 Executive summary

The one page to read if you read nothing else

Northgate's network works today because nothing has failed yet, not because it is designed to survive a failure. The firewall is one year from end of support, there is no backup of any configuration, a single ISP and a single firewall are both single points of failure for a clinic that cannot see patients without its EHR, and the staff Wi-Fi, guest Wi-Fi, and the lab analyzers all share one flat network. None of this is unusual for a practice this size. All of it is fixable in about 90 days without replacing the switches or access points.

OVERALL RISK

High

3 critical, 5 high, 6 medium findings

DEVICES IN SCOPE

47

1 firewall, 2 switches, 4 APs, 40 endpoints

END-OF-SUPPORT IN 12 MO

2

FortiGate 60E, 2017 PoE switch

FIX COST, 90 DAYS

\$9–14k

Hardware + labor, estimate, before any plan

What is working

- Internet, Wi-Fi, and the EHR are up during business hours; no outage reported in the last 6 months.
- FortiGate runs a supported FortiOS release (7.0.15) with IPS and web filtering licensed and on.
- Access points are a current model with 2 years of support left.
- Staff know who to call: one IT contact, one ISP contact, written on the rack.

What needs to change first

- **Back up the firewall config today** (F-01). There is no copy anywhere.
- **Close remote admin on the WAN side** (F-02). The firewall login page is reachable from the internet.
- **Separate guest Wi-Fi and lab devices from staff** (F-03). HIPAA risk analysis will ask for this.
- **Plan the FortiGate 60E replacement** before engineering support ends 2027-09-30 (F-04).

02 Scope and method

What we looked at and how

Site	One location, two floors, one telecom closet, one ISP (Comcast Business 300/35 Mbps, DOCSIS).
In scope	Firewall, switching, wireless, remote access, internet circuit, addressing, monitoring, backups of network configuration, physical closet, and the network-side controls a HIPAA risk analysis asks about.
Out of scope	Workstations, servers, EHR application, email, backups of patient data, printers. Noted where they touch the network.
Method	Read-only review of firewall and switch configuration; 7-day passive traffic and utilization capture via a temporary monitoring probe; Wi-Fi survey on both floors; 45-minute walkthrough with the office manager; vendor lifecycle lookup for every device.
Changes made	None. Assessments are read-only. One exception agreed on site: we exported the firewall configuration to encrypted storage so a copy exists (F-01).
Hours	9.5 of the 10 included in the Small Business tier.

03 Inventory and lifecycle

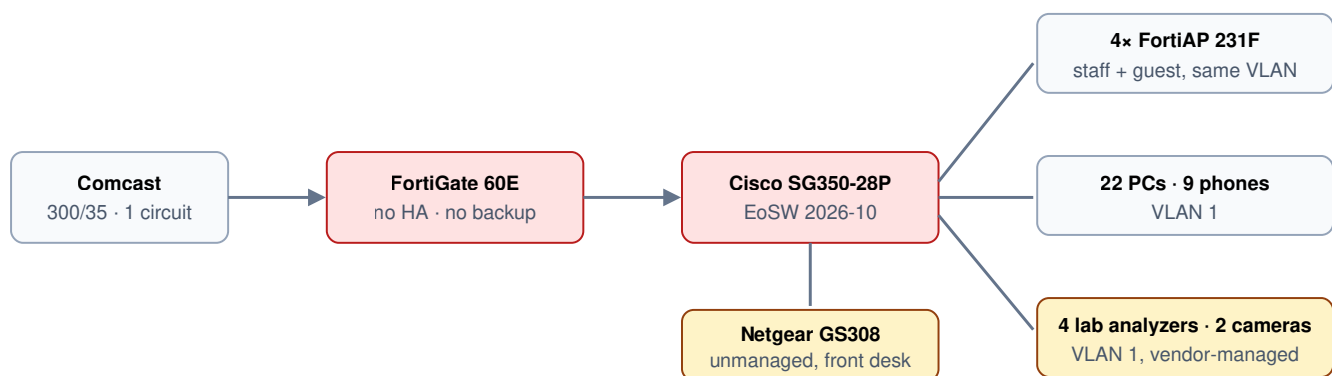
Every network device, with its vendor support status

DEVICE	MODEL	FIRMWARE	ROLE	SUPPORT ENDS	STATUS
fw-ngh-01	FortiGate 60E	FortiOS 7.0.15	Edge firewall, DHCP, DNS, VPN	2027-09-30 (EoES)	REPLACE IN 12 MO
sw-closet-01	Cisco SG350-28P	2.5.9.54	Core / PoE for APs, phones	2026-10-31 (EoSW)	END OF SOFTWARE
sw-floor2-01	Netgear GS308	unmanaged	8-port under front desk	n/a	UNMANAGED
ap-f1-lobby, ap-f1-exam, ap-f2-admin, ap-f2-exam	FortiAP 231F x4	7.0.5	Staff + guest Wi-Fi, managed by firewall	2029-03-31	SUPPORTED
ISP CPE	Comcast Business gateway	vendor	Bridge mode, single circuit	n/a	SINGLE ISP
Endpoints	22 PCs, 9 VoIP phones, 4 lab analyzers, 3 printers, 2 cameras	—	All on one VLAN	—	FLAT NETWORK

Lifecycle dates from Fortinet and Cisco product lifecycle pages, checked 2026-09-22. EoES = end of engineering support (no more security patches). EoSW = end of software maintenance.

04 Current topology

As found, with the single points of failure marked



Red = single point of failure or end of support. Amber = unmanaged or unsegmented.

Figure 1. Everything on the site depends on one circuit, one firewall and one switch, and every device can reach every other device.

05 Findings

14 findings, ranked by what happens if nothing is done

#	FINDING	SEVERITY	LIKELIHOOD	IMPACT IF IT HAPPENS	FIX EFFORT
F-01	No backup of firewall or switch configuration exists	CRITICAL	Certain on hardware failure	2–4 day rebuild from memory; VPN, DHCP, phones down	1 hr
F-02	Firewall admin (HTTPS, SSH) open on the WAN interface, password-only	CRITICAL	High; scanned daily	Full network compromise	1 hr
F-03	Flat network: staff, guest Wi-Fi, lab analyzers, cameras on one VLAN	CRITICAL	Medium	Guest or camera compromise reaches EHR workstations; HIPAA finding	2 days
F-04	FortiGate 60E end of engineering support 2027-09-30	HIGH	Certain	No security patches; cyber-insurance questionnaire fails	1 day + hardware
F-05	Cisco SG350 end of software 2026-10-31; already 2 CVEs unpatched	HIGH	Certain	Same as F-04 at the switch layer	1 day + hardware
F-06	Single ISP, no failover; EHR is cloud-hosted	HIGH	2 outages/yr typical for DOCSIS	Clinic cannot chart or bill during outage	½ day + \$60–90/mo LTE
F-07	SSL VPN in use for 3 remote users (Fortinet retiring SSL VPN; 7.0.x affected by multiple critical CVEs)	HIGH	High	Credential theft, remote access to LAN	½ day
F-08	DHCP pool 94% used on weekdays (7-day lease, no reservations)	HIGH	Monthly	Intermittent "can't get on the network"	1 hr
F-09	No monitoring or alerting; outages reported by staff	MEDIUM	—	Slow detection, no evidence for ISP disputes	½ day
F-10	Unmanaged 8-port switch feeds 6 front-desk devices	MEDIUM	—	No visibility, cannot segment	Replace, ½ day
F-11	Firewall local admin account shared; no MFA; no logging retained beyond 7 days on-box	MEDIUM	—	No audit trail for HIPAA	2 hr
F-12	Wi-Fi: 2.4 GHz channel overlap, lobby AP at 100% power, dead spot in exam 6	MEDIUM	—	Tablets drop during intake	2 hr
F-13	Closet: no UPS on switch; firewall UPS battery dated 2021	MEDIUM	—	Every blip is a 4-minute outage	\$300, 1 hr
F-14	No written network documentation; cabling unlabeled	MEDIUM	—	Slower every future repair	Produced by this report

F-01 · No configuration backup

Evidence: firewall "config backup" never run (no revision history on-box); switch has no TFTP/SCP target; office manager confirmed no copies. Verified 2026-09-16.

Why it matters. The firewall holds 41 policies, the DHCP scopes, the DNS overrides for the EHR vendor, 3 VPN users and the AP profiles. If the 60E fails, which is likely in its last year, a replacement arrives blank. Rebuilding from memory takes days and will not match.

Fix. Enable scheduled encrypted backup to off-site storage (FortiGate supports this natively, or via a config-backup tool such as Oxidized that keeps a versioned history). Done during this assessment as a one-off export. Ongoing: 1 hour to set up, then automatic.

F-02 · Administrative access exposed to the internet

Evidence: WAN interface allows HTTPS and SSH (set allowaccess ping https ssh); login reachable from an outside address on 2026-09-15; FortiAnalyzer not present so failed-login history is 7 days only: 1,412 failed logins in that window from 63 addresses.

```
config system interface
  edit "wan1"
    set allowaccess ping https ssh      <-- exposed
    set ip 203.0.113.42 255.255.255.248
  next
end
config system admin
  edit "admin"
    set trusthost1 0.0.0.0 0.0.0.0      <-- any source
    # no two-factor configured
  next
end
```

Fix. Remove HTTPS/SSH from the WAN interface; restrict admin to the management VLAN and the Ambio management tunnel; add a trusted-host list; enable FortiToken MFA for the admin account; move "admin" to a named account per person. One hour, no downtime.

F-03 · One flat network for staff, guests, lab equipment and cameras

Evidence: single VLAN 1 (192.168.1.0/24) on every switch port and both SSIDs; guest SSID differs only in password; 4 lab analyzers run vendor-managed Windows 7 embedded and cannot be patched; 2 IP cameras use default credentials.

Why it matters. A patient's phone on guest Wi-Fi, or a camera with a default password, can reach every EHR workstation. The HIPAA Security Rule risk analysis your compliance consultant runs will list this. So will your cyber-insurance renewal.

Fix. Four VLANs: Staff, Guest (internet only), Clinical devices (analyzers, allowed only to their vendor cloud), and Management. Firewall policies between them, default deny. Requires the managed switch to be configured (or replaced, see F-05) and a 2-hour after-hours cutover. Guest and camera isolation can be done first, in one evening, on the current hardware.

Days 1–30 · Stop the bleeding

- F-01 config backups (done once; make it automatic)
- F-02 close WAN admin, add MFA
- F-08 DHCP lease 12 h + reservations
- F-07 move 3 VPN users from SSL VPN to IPsec or ZTNA
- F-13 UPS battery, add UPS to switch
- F-03 guest and camera isolation only

Est. \$1,200–1,800 labor, \$300 hardware. No business-hours downtime.

Days 31–60 · Fix the foundation

- F-05 replace SG350 + Netgear with one 48-port PoE managed switch
- F-03 full segmentation (4 VLANs) during switch cutover
- F-09 monitoring and alerting (uptime, bandwidth, device health)
- F-12 Wi-Fi channel/power plan; move lobby AP
- F-11 named admin accounts, log retention off-box

Est. \$4,500–6,500 incl. switch (\$2,200–3,000). One 3-hour after-hours cutover.

Days 61–90 · Remove the single points of failure

- F-04 replace FortiGate 60E with FortiGate 70G + 3-yr UTP (sized for 300 Mbps with IPS on)
- F-06 add LTE/5G backup circuit with automatic failover
- F-14 as-built documentation, labeled cabling, rack photo
- Hand-off: runbook, credentials in a vault, monitoring access

Est. \$3,500–5,500 incl. firewall + licensing, plus \$60–90/mo LTE. One 2-hour evening cutover.

Estimates are ranges from list pricing on 2026-09-22 and the labor hours in this report. A fixed-price statement of work follows if you choose to proceed; you are not obliged to. Option: a redundant firewall pair (HA) adds about \$2,400 and removes the last single point of failure except the building's power.

08 What you own after this report

*Deliverables, whether or not we work together again***Included with this report**

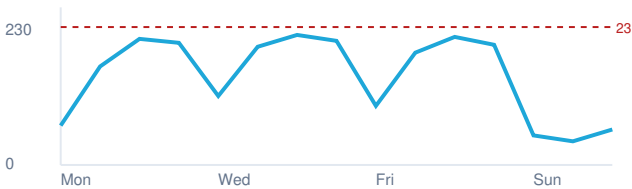
- This document, PDF, yours to give to any vendor
- Device inventory spreadsheet with serials, firmware, support dates
- Current-state network diagram (Figure 1) as editable file
- Encrypted export of the firewall configuration (F-01), key held by you
- Wi-Fi survey heat maps, both floors
- 7-day utilization and uptime capture, raw data

How the assessment was scored

- **Severity:** what happens if nothing is done. Critical = outage or breach with no workaround. High = outage or compliance finding with a workaround. Medium = degraded service or cost.
- **Likelihood:** based on vendor lifecycle dates, observed events in the 7-day capture, and published exploitation of the specific software versions.
- **Effort:** hours for a senior engineer, including testing and rollback plan.

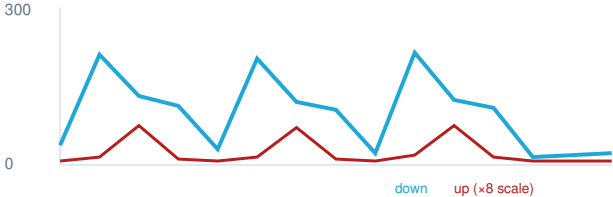
DHCP pool utilization, 7 days (F-08)

Pool 192.168.1.20–.250 (231 addresses). Peak 218 leases Tue 10:40.



Internet circuit utilization (F-06)

300 Mbps down. Peak 212 Mbps during 08:00–09:00 EHR sync. 35 Mbps up saturated 4 times (camera uploads).



Prepared by Jeff Johnson, Ambio IT Solutions LLC dba Ambio Edge Networks. Cisco, Fortinet and CompTIA certified. Fortinet Engage Advocate partner. This sample is published at ambioedge.com so prospective customers can see exactly what the Network Risk Assessment produces before they buy one.