Network segmentation: can one infected laptop reach everything?

This quarter, move hypervisor, backup and device management into a zone reachable only from admin workstations, and block SMB, RDP and WinRM between workstations with the host firewall. Then put a default-deny firewall between users and servers one zone at a time, and count a rule as working only once you have tested it from a user's laptop.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.1**

Written for

IT and network teams with flat or lightly segmented office networks, on-premises servers, some cloud and, in some cases, OT or building systems

Latest version

sheets.einblick.dev/network-segmentation/

If you only do five things

1. **Wall off the management plane first.**
   Put hypervisor and storage management, server controllers such as iLO and iDRAC, and backup consoles in segments only an admin subnet can reach. M-Trends 2026 says to treat virtualization and management platforms as Tier 0[1]. Google saw attackers use a Cisco CIMC controller to overwrite a backup cluster's operating system[2].
2. **Stop workstations talking to each other.**
   With Windows Firewall policy from Group Policy or Intune, let workstations accept SMB and RPC (TCP 135, 139, 445), RDP (3389), WinRM (5985, 5986) and WMI only from admin and management hosts[3]. Scope the allow rules rather than adding block rules, which override any allow rule they overlap[7]. RDP carried lateral movement in about 85% of Google's 2025 ransomware cases[2].
3. **Put a default-deny firewall between users and servers.**
   BSI requires clients and servers in separate segments with at least a stateful firewall between them[5]. Domain controllers and file servers usually need to be reachable from across the network[6], so open only their service ports.
4. **Deny server egress by default.**
   Servers, hypervisors, network devices and OT should reach only allow-listed destinations, such as update servers. Mandiant advises this deny-by-default model, plus blocking recursive DNS lookups that aren't on an allow-list[3].
5. **Test the rules from where an attacker stands.**
   Every quarter and after each firewall change, scan from a user laptop and the guest network toward the management, backup and server zones. Alert on rule changes: in one 2025 intrusion, attackers created firewall policies that gave them access to more subnets[2].

Segment a flat network in this order

1. **Map what talks to what.**
   Collect a month of firewall or flow logs, so monthly jobs show up. CISA advises building each system's dependency list from observed traffic and checking it with its owners[4].
2. **Build the management zone and the admin path.**
   Reach it only from a privileged access workstation (PAW) subnet, and remove every direct route from the user LAN[3].
3. **Add rules that allow and log.**
   Put servers and user groups behind the internal firewall with logging rules, to see what default deny would break. CISA calls this permissive mode[4].
4. **Enforce default deny, one zone at a time.**
   Allow the flows you saw, deny the rest and keep a rollback ready[4]. Start with your IT team's own devices, as Microsoft suggests for SMB rules[6].
5. **Test, then move to the next zone.**
   Scan from each zone into the others and compare the result with the plan. BSI requires regular checks that the live network matches it[5].

Zones to create, and what may cross them

- **Management.** Hypervisor, storage and switch management, server controllers and the PAW subnet. Put infrastructure VLANs in their own VRF so user and guest zones have no route to them, and vMotion and storage traffic on non-routable VLANs[3]. The edge devices sheet covers firewall and VPN management.
- **Backups.** Non-routable VLANs, with console access only from a PAW and with phishing-resistant MFA[3]. The ransomware sheet covers the copy attackers can't delete.
- **Identity.** Domain controllers and certificate authorities, both Tier 0 for Mandiant[3]. Clients get the directory ports they need, including RPC on TCP 49152-65535[8]; admin protocols come only from PAWs.
- **Servers.** Group them by application and data sensitivity, and keep development apart from production[4].
- **Guest, IoT, printers and building systems.** Give them dedicated segments, as BSI requires for guest access and devices you don't control well[5], with access only to the internet or the one server they report to. The 2026 DBIR recounts the Akira group encrypting network shares from an unsecured webcam, unseen by Windows EDR[15].
- **Cloud.** Give each tier its own security group that accepts traffic only from the group in front of it, and remove the allow-all outbound rule that new AWS security groups start with[13]. Keep Kubernetes API servers on private endpoints[3].

OT and building systems

- **Keep OT running when IT is down.** End IT access in an OT DMZ, and give OT its own AD forest and its own backup, EDR and jump servers[3].
- **Let OT start every connection.** Vendors come in through a broker in the DMZ, and IT reads a historian copy there, not the OT systems[10].
- **Use zones and conduits.** Group assets with the same security needs into zones and control the paths between them, as IEC 62443 does. First find every data flow, including radio links missing from the diagrams[10]. ACLs are the minimum control between zones[10].

Check that the rules hold

- **Port-scan from the user side.** Anything that answers beyond the documented ports is a finding.
- **Log what host firewalls drop.** Send dropped-packet logs from hypervisors and management hosts to your SIEM: denials there signal reconnaissance[3].
- **Stop local exceptions.** Turn off local rule merging[3]. Apps then need central rules, and local Group Policy rules still apply[7].
- **Meet the card data clock.** If segmentation isolates your card data environment, PCI DSS v4.0.1 requires pen tests of it at least every 12 months (6 for service providers) and after changes[12].

What changed in 2026

- **Handoffs now take seconds.** M-Trends 2026 found the median handoff from initial access to a second group fell to 22 seconds in 2025, from more than 8 hours in 2022[1]. Close lateral paths before an incident.
- **Eight agencies set OT connectivity principles.** The January 2026 principles call for connections that start inside OT, a hardened OT boundary and a tested isolation plan[10].
- **Critical infrastructure got isolation guidance.** CI Fortify (July 2026) covers mapping vital systems and building separation points, so vital OT can be cut off from all other networks in a crisis and keep running[11].
- **New Azure networks are private by default.** VNets created with API versions released after 31 March 2026 have no default internet egress. Existing VNets and older API versions keep it[14].

What you can skip

- **Full microsegmentation before basic zones.** CISA warns that fine-grained segments are harder to build and maintain, and its on-premises example did data center, servers and users first[4].
- **VLANs without rules between them.** A VLAN with no default-deny firewall or ACL in front of it is a label, not a segment.
- **Default-deny outbound on workstations.** Microsoft advises allowing outbound in most deployments[7]. Block SMB to the internet at the edge[6].
- **Deep inspection between internal zones.** Stateful port rules do most of the work. Inspect at the internet edge and the OT boundary first.

Mistakes that cost the most

- **A management side door.** One management switch or jump server that reaches every layer bypasses the firewalls between them. The NCSC calls this management bypass[9].
- **Admin work from everyday laptops.** Administering systems from a device less trusted than they are is another NCSC anti-pattern[9].
- **Shared tools across zones.** Backup, EDR and jump servers that span IT and OT connect what you separated[3].
- **Temporary rules that stay.** Give every allow rule an owner, a ticket and a review date.

What this looks like at your size

Small team, no security staff

- From Intune or Group Policy, disable the File and Printer Sharing, Remote Desktop and WinRM firewall rules on laptops.
- Put guest Wi-Fi, cameras and building systems on their own VLANs with internet access only.
- Move hypervisor, NAS and backup admin interfaces to a VLAN only one admin device can reach.
- Ask your IT provider what a user laptop can reach.

Growing, with IT or security staff

- Build management, backup, identity and server zones, logging before you enforce.
- Give admins PAWs or a hardened jump host.
- Deny server egress except to allow-listed update and service endpoints.
- Scan from each zone every quarter and after firewall changes.

Enterprise or regulated

- Keep a flow inventory per application with an owner, and review the rules yearly.
- Pilot microsegmentation where agents or cloud security groups can follow the workload.
- Separate OT with a DMZ and its own identity, and test the isolation plan.
- Schedule PCI DSS segmentation tests; in Germany, map zones to BSI NET.1.1.

Version history

5 Nov 2026, version 1.1 Reviewed for company readers: laptop firewall rules are set from Intune or Group Policy.

Sources

1. M-Trends 2026: Data, Insights, and Strategies From the Frontlines. Google Cloud (Mandiant), 23 Mar 2026. cloud.google.com
2. Ransomware Under Pressure: Tactics, Techniques, and Procedures in a Shifting Threat Landscape. Google Threat Intelligence Group, 16 Mar 2026. cloud.google.com
3. Proactive Preparation and Hardening Against Destructive Attacks: 2026 Edition. Google Cloud (Mandiant), 6 Mar 2026, updated 13 Mar 2026. cloud.google.com
4. Microsegmentation in Zero Trust, Part One: Introduction and Planning. CISA, 29 Jul 2025. cisa.gov
5. IT-Grundschutz NET.1.1 Netzarchitektur und -design. BSI, Edition 2023. bsi.bund.de
6. Secure SMB Traffic in Windows Server. Microsoft Learn, 25 Oct 2024. learn.microsoft.com
7. Windows Firewall rules. Microsoft Learn, 6 Jun 2025. learn.microsoft.com
8. Configure firewall for AD domain and trusts. Microsoft Learn, 12 Feb 2026. learn.microsoft.com
9. Security architecture anti-patterns. NCSC (UK), version 1.0, 22 May 2019. ncsc.gov.uk
10. Secure connectivity principles for operational technology (OT). NCSC (UK) and seven partner agencies, 14 Jan 2026. ncsc.gov.uk
11. CI Fortify: Advice for isolating vital systems. CISA and ASD's ACSC, 28 Jul 2026. cisa.gov
12. PCI DSS v4.0.1, requirements 11.4.5 and 11.4.6. PCI Security Standards Council, Jun 2024. pcisecuritystandards.org
13. Security group rules (Amazon VPC User Guide). AWS Documentation, checked 3 Nov 2026. docs.aws.amazon.com
14. Default outbound access in Azure. Microsoft Learn, 24 Jul 2026. learn.microsoft.com
15. 2026 Data Breach Investigations Report (Year in review). Verizon, 19 May 2026. verizon.com