I

Intranet: How It Works, Examples, and Security Controls

Learn how intranets differ from the Internet and extranets, how remote access works, and why internal network location should not automatically grant trust.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 Is an intranet the same as a local network?

02 Intranet vs. Internet vs. extranet

03 Common intranet services

04 How users access an intranet

05 Intranet security controls

06 Why HTTPS is needed internally

07 Zero trust and the intranet

08 Common intranet risks

09 Intranet troubleshooting checklist

An **intranet** is a private network or collection of internal services an organization uses for employees, applications, documents, and workflows. It commonly uses the same web, DNS, identity, and network technologies as the public Internet but limits access to authorized users and devices.

“Internal” does not mean inherently secure. Compromised accounts, infected endpoints, contractors, cloud integrations, and configuration errors can all place an attacker inside the traditional perimeter.

01 Is an intranet the same as a local network?

Not exactly. A local area network (LAN) describes a network with limited geographic scope, such as an office or building. An intranet describes private organizational services and their access policy. An intranet can span many offices and cloud environments, and remote employees may reach it across the public Internet through a VPN or identity-aware gateway.

02 Intranet vs. Internet vs. extranet

- The **Internet** is the global network of interconnected public and private networks.
- An **intranet** provides internal organizational resources.
- An **extranet** exposes a controlled subset of resources to partners, suppliers, or customers.

The same application can have separate public and internal interfaces. Access policy, not the hostname alone, determines who should reach each interface.

03 Common intranet services

Examples include employee portals, policy libraries, ticketing, internal documentation, HR tools, dashboards, source-code platforms, file shares, directory services, and administration consoles. Some run on premises, while others are private cloud services or software-as-a-service applications connected to company identity.

04 How users access an intranet

Office users may connect through a local network. Remote users commonly use a VPN, zero-trust network access service, application proxy, or identity-aware gateway. Access should authenticate the user and device and evaluate the requested resource. Connecting to a VPN should not automatically grant unrestricted access to every internal subnet.

05 Intranet security controls

1. Use centralized identity, MFA, and role-based least privilege.
2. Segment users, servers, administrators, and sensitive systems.
3. Encrypt web and application traffic, including internal connections.
4. Patch internal services and remove unsupported systems.
5. Restrict administration to dedicated accounts and paths.
6. Log authentication, access, changes, and data exports.
7. Back up critical content and test restoration.

06 Why HTTPS is needed internally

Internal traffic can cross Wi-Fi, shared infrastructure, proxies, virtual networks, and compromised segments. TLS protects credentials and content in transit and authenticates the service name. Use managed internal certificate authorities or trusted public certificates; teaching users to ignore certificate warnings weakens the entire environment.

07 Zero trust and the intranet

NIST zero-trust guidance focuses protection on users, devices, and resources rather than treating network location as the main source of trust. Apply explicit authentication and authorization to each important service, continuously reassess access, and limit lateral movement. Zero trust does not mean removing firewalls or exposing every internal application publicly.

08 Common intranet risks

- Old applications reachable by every employee device.
- Shared administrator passwords and broad file permissions.
- Internal DNS names or documents accidentally indexed publicly.
- Extranet accounts retaining access after a partnership ends.
- Secrets stored in wikis, scripts, tickets, or shared folders.
- No monitoring because traffic is assumed to be trusted.

09 Intranet troubleshooting checklist

Confirm network or remote-access status, DNS resolution, system time, TLS trust, identity, group membership, and application health. Test the exact hostname rather than substituting an IP address, which can break TLS and virtual-host routing. If access unexpectedly expands or sensitive content becomes public, preserve logs and treat it as a security incident.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com