S

Screened Subnet Firewall: Architecture, DMZ Rules, and Examples

A screened subnet firewall places a DMZ between the internet and an internal network. Learn its architecture, traffic rules, advantages, limitations, and deployment checks.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 Screened subnet components
02 One-firewall and two-firewall designs
03 Screened subnet vs screened host
04 Typical traffic rules
05 What belongs in the DMZ?
06 Advantages and limitations
07 Deployment checklist
08 Home-router DMZ is not the same design
09 Frequently asked questions

A **screened subnet firewall** is a network architecture that places a perimeter network between an untrusted network, usually the internet, and a protected internal network. The perimeter network is commonly called a **DMZ**. Public-facing systems can be reached in the DMZ without providing a direct route to internal workstations and data.

The design creates three security zones:

```
Internet → external filtering → DMZ → internal filtering → LAN
```

If a public server is compromised, the attacker must still cross a separately controlled boundary to reach the internal network.

01 Screened subnet components

- **External network:** the internet or another untrusted network.
- **External firewall or screening router:** permits only intended traffic to systems in the DMZ.
- **Perimeter network or DMZ:** contains exposed services and tightly controlled intermediaries.
- **Bastion host:** a hardened system designed to receive untrusted connections, such as a reverse proxy, mail relay, DNS server, or secure gateway.
- **Internal firewall or screening router:** restricts traffic between the DMZ and the protected LAN.
- **Internal network:** user devices, application services, management systems, and sensitive data that should not be directly internet-accessible.

02 One-firewall and two-firewall designs

Design	How it separates zones	Trade-off

Three-legged or triple-homed firewall	One firewall uses separate interfaces for internet, DMZ, and LAN.	Simpler and less costly, but one device and rule set enforce both boundaries.
Dual-firewall screened subnet	An external firewall separates the internet from the DMZ; an internal firewall separates the DMZ from the LAN.	Stronger separation and the option to use different technologies, with more cost and operational complexity.

Physical appliances are not required. Cloud networks can implement the same logical pattern with separate subnets, routing tables, security groups, network firewalls, and identity-aware gateways.

03 Screened subnet vs screened host

A **screened host** design uses a filtering router and one hardened bastion host associated with the internal network. A **screened subnet** creates a distinct perimeter network for one or more bastion hosts. The separate DMZ provides another boundary and reduces direct exposure of the LAN.

The terms are sometimes used inconsistently. Verify the actual zones, routes, and enforcement points instead of relying only on a vendor's "DMZ" label.

04 Typical traffic rules

Traffic direction	Recommended default	Example exception
Internet → LAN	Deny.	None; publish a service through the DMZ instead.
Internet → DMZ	Deny except explicitly published services.	HTTPS to a reverse proxy or authoritative DNS to a DNS server.

Traffic direction	Recommended default	Example exception
DMZ → LAN	Deny except narrowly required application flows.	A reverse proxy to a specific application server and port.
LAN → DMZ	Allow only required user and management paths.	Administration through a dedicated jump host.
DMZ → Internet	Restrict and log.	Operating-system updates, DNS resolution, or a defined upstream API.
LAN → Internet	Apply organizational egress policy.	Web access through a controlled gateway.

Use source and destination identities, addresses, ports, applications, and direction when the platform supports them. "Any to any" rules defeat the value of the architecture.

05 What belongs in the DMZ?

- Reverse proxies, web application firewalls, and load balancers.
- Public web front ends that do not store unnecessary sensitive data.
- Authoritative DNS servers, mail relays, VPN gateways, and secure file-transfer gateways.
- Jump hosts or management proxies when they are hardened, strongly authenticated, and not exposed broadly.

Domain controllers, user workstations, databases containing sensitive records, backup controllers, and broad administrative tooling should not be placed in the DMZ merely for convenience.

06 Advantages and limitations

Advantages

- Prevents direct internet connections to the internal network.

- Limits lateral movement after compromise of a public service.
- Provides clear points for logging, inspection, rate limiting, and access control.
- Allows public services to be maintained separately from internal systems.

Limitations

- A permissive DMZ-to-LAN rule can turn the perimeter server into a direct path inward.
- The design does not patch or harden the systems placed in it.
- Stolen administrator credentials can bypass the intended network boundary.
- Unknown routes, wireless links, cloud peering, or management networks can create side doors around the firewall.
- More zones and devices increase configuration and monitoring work.

07 Deployment checklist

1. Inventory every public service and remove exposure that is not required.
2. Assign separate address ranges, routes, and security policy to internet, DMZ, management, and internal zones.
3. Start with default deny and document the owner and purpose of each exception.
4. Prevent direct administrative access from the internet; use a VPN, identity-aware proxy, or controlled jump path with MFA.
5. Use separate service accounts and secrets for DMZ systems. Do not grant them broad internal privileges.
6. Filter outbound DMZ traffic so a compromised host cannot connect anywhere it chooses.
7. Centralize firewall, authentication, DNS, endpoint, and application logs outside the DMZ.
8. Review rules and routes regularly and test whether prohibited paths are actually blocked.

08 Home-router DMZ is not the same design

A consumer router's "DMZ host" option often forwards nearly all unsolicited inbound traffic to one internal device. It does not necessarily create a separate screened subnet. Enabling that option can expose the selected device and should not be confused with an enterprise perimeter network.

09 Frequently asked questions

Is a screened subnet the same as a DMZ?

The terms are often used as synonyms, but usage varies. A screened subnet specifically emphasizes a perimeter subnet protected from both the external and internal networks. Confirm how the product implements interfaces, routing, and filtering.

Does a DMZ need two firewalls?

No. A single firewall with three or more isolated interfaces can create internet, DMZ, and LAN zones. Two firewalls can provide additional separation but also require consistent operations and monitoring.

Can the DMZ connect to an internal database?

Only when the application requires it, and then through a narrowly defined destination, port, identity, and encrypted protocol. A safer design may place an application tier between the public front end and sensitive data.

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