Segmentation

- Network Layout
- Trusted
- Servers
- IoT
- DMZ
- Agents

Network Layout

Network Segmentation

The home network is split into separate vlans. Each zone holds devices with a similar purpose and level of trust. A firewall sits between the zones and decides which traffic may cross. Anything not explicitly allowed is blocked.

VLAN Zones

Trusted

Personal computers and phones used by people on site.

- Can reach every other zone and the internet.
- Is the only zone from which internal management interfaces are reachable.

Servers

Infrastructure and internal services.

- Cannot initiate connections into the Trusted zone.
- Cannot initiate connections into the DMZ.
- Can reach the IoT zone and the internet.
- Hosts name resolution and the internal applications.

IoT

Smart-home and other low-trust devices.

- Internet access only.

- Cannot reach any internal zone.
- Allowed only the basic services it needs to function (name resolution and time sync).
- Accessible through mDNS repeater

DMZ

The zone for anything reachable from the internet.

- Isolated from the Trusted and Servers zones.
- Allowed to reach only the specific application services it fronts, and nothing else.
- Management of its hosts is initiated from inside, so no inbound path into internal zones exists.

Agents

Automation and AI agent hosts.

- Internet access only.
- Cannot reach any internal zone.
- Agents operate in strict sandbox

Planned zones

- **Guest:** visitors' devices, internet only. *Planned, not built.*
- **Cameras:** no internet access. *Planned, not built.*

Design rules

1. **Default deny.** Traffic is blocked unless a rule allows it.
2. **Least privilege.** Each zone gets only the access its purpose needs.
3. **Services reachable from outside sit in their own zone,** apart from the internal network.
4. **Remote access uses a VPN,** and the VPN reaches only the zones it needs.
5. **Safe if known.** The design is meant to hold even if every detail is public, so it relies on hardening, not secrecy.

How it's verified

See the Verification book for tests that show the rules work, such as an isolated zone timing out when probed from another.

Trusted

Network for personal devices used by people: laptops, phones and tablets. Accessible only in person on site.

Permitted devices

Currently, all devices that are used regularly are allowed on the Trusted network. Devices should be signed in and actively used. Main use case are for computers, phones, and tablets. High-risk devices such as smart TVs and smart devices are connected via IoT

Access

Devices on Trusted **can** reach:

- Every other zone.
- The internet

Devices on Trusted **cannot** reach:

- Nothing is blocked from this zone

Notes

- It is the only zone from which internal management interfaces can be reached.
- Other zones cannot start connections into it. They can only reply to connections it starts.

Why it is designed this way

Network admins use these devices and need broad access. Additionally, high trust of client's devices ensures maximum connection reliability. The protection comes from the other zones being unable to reach back into this one. Plan in the future to split this vlan into end-user devices and management devices so compromised client devices pose less risk.

Related

- Rules by Zone

Servers

Network for infrastructure and internal services that run all the time. Not meant for everyday use by people.

Permitted devices

The virtualization and container hosts, the internal applications that run on them, and shared infrastructure such as name resolution. Hosts are added here only if they provide a service to the rest of the network.

Access

Servers can reach the IoT network and the internet. They can't start connections into Trusted or the DMZ.

Notes

- A host that sits in more than one zone runs its own firewall as a second layer.
- Servers can still reply to connections that start elsewhere. The block only applies to outbound traffic.

Why it's set up this way

Devices on the server network are accessed by many guests. Compromising a device on this network shouldn't enable access to the rest of the network. If a server is compromised, it still can't start connections into Trusted or the DMZ.

IoT

Network for smart-home and other low-trust devices.

Permitted devices

Smart plugs, sensors, speakers, smart TVs and similar devices. If I can't patch it or can't see what its software does, it goes here. These devices also tend to be lacking in security and control.

Access

IoT can reach the internet, plus the basics it needs to work: name resolution and time sync. It can't reach any internal zone. Select internal devices are able to start connections to IoT

Notes

- Devices here only reach out to the internet. Nothing in this zone can start a connection to another zone.
-

Why it's set up this way

These devices are the most likely to be compromised and the hardest to secure. With internet access only, a compromised gadget can't reach personal devices or servers. Devices on this network are set up with an "already compromised" framework.

DMZ

Network for anything that has to be reachable from the internet. Acts as a buffer zone between WAN and the internal network.

Permitted devices

Only hosts that sit in front of public services. They accept connections from outside and pass them on to the right internal application. Nothing else lives here.

Access

The DMZ can reach the specific application services it fronts, and the internet for certificates and updates. It can't reach Trusted, and it can't reach the rest of Servers. Requires granular firewall management.

Notes

- DMZ hosts are managed from the inside. The connection starts from within the network, so there is no inbound path from the DMZ into the internal zones.
- New public services get published through this zone, never straight from an internal one.

Why it's set up this way

Anything exposed to the internet gets attacked first. Keeping it isolated means a compromise here doesn't hand over the rest of the network. In the future, consider a dual-dmz setup.

Agents

Network for hosts that run automation and AI agent software.

Permitted devices

Machines that are managed by/host agents. Nothing else shares this zone. Services used by the agents (non-root) are hosted on other networks and accessed over the internet.

Access

Agents can reach the internet, plus name resolution and time sync. They can't reach any internal zone.

Notes

- Everything an agent does goes out through the internet. Nothing it does can start a connection to another zone.

Why it's set up this way

Agent software takes actions on its own and talks to outside services, so it is treated as an untrusted guest. If one misbehaves or gets manipulated, it can't touch personal devices or servers.