Micro Segmentation

Secure network communication within the data center

Network — Is secured with → App Security Policies

App Security Policies — Are set on → App Type Categories

App Type Categories — Can have multiple → Tiers — Are → Separate layers of the application architecture
e.g. Web, Database

App Type Categories — Can be filtered by → A separate category — Can be → Environment, location, department, etc.

App Security Policies — Regulate → Inter-App Traffic

Inter-App Traffic — Consists of → Inbound Rules — Specify allowed → Sources — Can be → All sources / No sources / Specific sources

Sources — Talk to app via → Ports & Protocols

Specific sources — Can be → Categories / IPs / Subnets

Inter-App Traffic — Consists of → Outbound Rules — Specify allowed → Destinations — Can be → All destinations / No destination / Specific destinations

Destinations — Talk to app via → Ports & Protocols

App Security Policies — Regulate → Intra-App Traffic — Consists of → Tier-to-Tier Rules — Specify allowed → Tiers

Tiers — Talk to each other via → Ports & Protocols

Between / Between app and / Between app and

App Security Policies — Support use of → Service Chains — Can be inserted

Service Chains — Are sequences of → Network Services — Can be → Firewalls / Deep Packet Inspection / Access Control / etc.

App Security Policies — Can be → Monitored before applying

One Quarantine Policy — Isolates → Individual VMs

One Quarantine Policy — Can have → Inbound Rules — Specify allowed → Sources — Can be → No sources / Specific sources (forensic tools)

Sources — Talk to quarantined via → Ports & Protocols

Specific sources (forensic tools) — Can be → Categories / IPs / Subnets

One Quarantine Policy — Can have → Outbound Rules — Specify allowed → Destinations — Can be → No destination / Specific destinations (forensic tools)

Destinations — Talk to quarantined via → Ports & Protocols

One Quarantine Policy — Is → Applied

Isolation Policies — Isolates → Two VM categories

Is denied between

Isolation Policies — Denies → Inter-category traffic

Isolation Policies — Can be → Monitored before applying