Understanding Micronets

Darshak Thakore
Principal Architect, Security Technologies
CableLabs
Vision

“Re”design on-premise networks

• Ease of use
• Automated service management
• Integrated security controls
Core Capabilities

- Network premises segmentation
- Separate trust domains
- Flow (traffic) management
- Visibility
- Dynamic rules/policy management
  - Leveraging identity of each endpoint
  - Device granular malware management (sand boxing)
“Micro” Segmentation

1. Micronets gateway segments network into trust domains
2. Micronets manager maps devices into trust domains
3. SDN enforces and controls switching and routing
4. User has control to the degree they want
5. Security threats contained to a micronet or can be quarantined

Micronets management microservices

Internet service provider

Micronets gateway

Quarantined network

Automobile management

Health

Home security

Home automation
Secure Connectivity

Micronets gateway segments network into trust domains

Micronets manager maps devices into trust domains

SDN enforces and controls switching and routing

User has control to the degree they want

Secure connectivity is configured and updated as necessary
Reference Architecture

Service Provider Components

- Micronets microservices layer
  - Intelligent services and business logic (including AI based services)

Partners and Service Providers

- Micronets APIs
- Healthcare provider

On-premise Network

- Managed Services Micronets
- Customer Micronets (automatically organized, with manual overrides)

Access and Core Network

Gateway

Secure connection (automatically established after provisioning and on-board of device)

Service management
• Open Source Code
  • cablelabs.github.io/micronets

• Gateway components
• PoC microservices
• Device onboarding

• Common AI/ML API’s
• Specification Work
• WFA, IETF
• It’s happening – sign up for future Micronets updates at https://go.cablelabs.com/micronets

• Questions:
  • Email: d.thakore@cablelabs.com
Questions?