# OpenBSD IPSec Configuration (host-to-host)


CENTRAL
MISSISSIPPI

# References

- OpenBSD FAQ - Virtual Private Networks (VPN)
  - https://www.openbsd.org/faq/faq17.html
- Man pages:
  - iked(8)
  - ikectl(8)
  - iked.conf(5)
  - ipsecctl(8)
  - rcctl(8)

# Introduction

- OpenBSD comes with iked(8), a modern, privilege-separated IKEv2 server
  - It can act both as responder, e.g. a server receiving connection requests, or initiator, e.g. a client initiating a connection to a responder
  - The ikectl(8) utility is used to control the server, which gets its configuration from the iked.conf(5) file

# Agenda

- Configuration (iked.conf)
- Start iked on both endpoints for testing
- Verify IPsec flows (ipsecctl)
- Configure the iked service for continuous operation

# Configuration

- Ownership and permissions for /etc/iked.conf
- Sharing public keys between nodes
- Mapping public keys to automatic keying policies

# Start iked

- Run iked on the endpoints with debugging:
  - “iked -dv”

# Verify IPsec Flows

- View the IPsec flows:
  - “ipsecctl -sa”
- Confirm with tcpdump
  - Primary interface
  - enc0 interface

# Configure Continuous Operation

- Service configuration commands:
  - rcctl enable iked
  - rcctl start iked


CENTRAL
MISSISSIPPI

# Comments/Questions

# Backup slides

CENTRAL MISSISSIPPI