



PRESENTS

**NETWORLD INTEROP**

an INTEROP event

# IPSEC versus SSL

---

**Moderator:** Alistair Croll

**Participants:** Gorka Sadowski, NetScreen

Randy Smerik, Intel

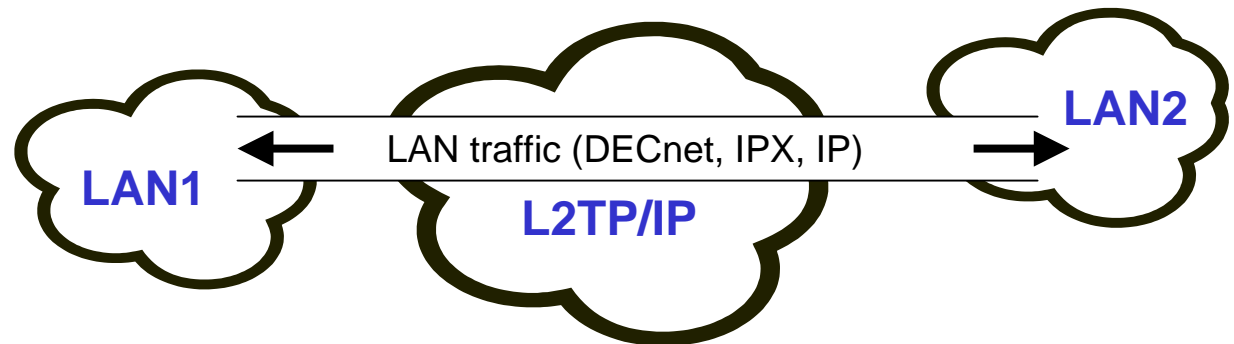
Bill Miller, Andes Networks

2:00 – 3:15 PM, September 13, 2001

# Network-to-network security (L2F)

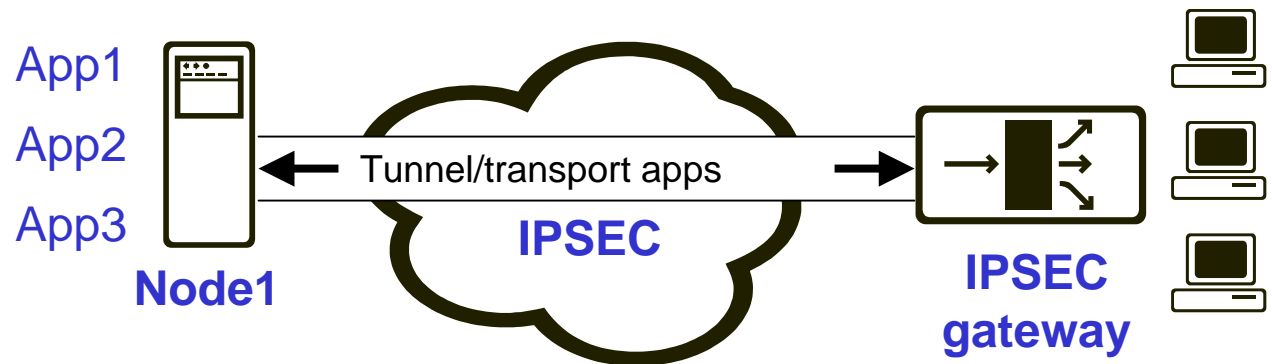
---

- Establish a layer 2 tunnel between sites
- Control access between LANs
- All applications can travel between all nodes on the LANs at either end
- Generally needs password exchange beforehand
- **Good for office-to-office or extranet partners with non-IP traffic, usually one-to-one**



# Node-to-node security (IPSEC)

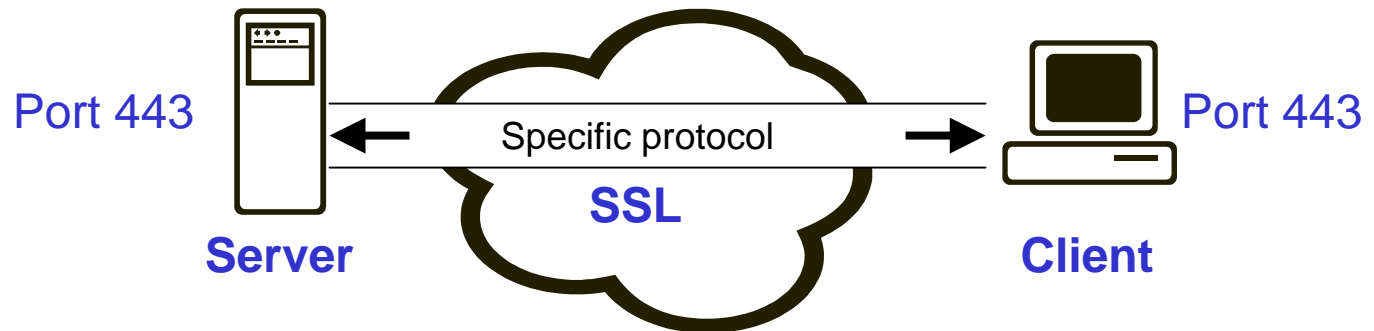
- Firewalling according to address ranges
- IPSEC to encrypt traffic
- May use a public key infrastructure to authenticate
- May be one-to-one (office-to-office) or many-to-one (remote access)
- Any TCP ports flow over the IPSEC tunnel
- Visitor probably established identity before visiting



# Application-to-application security (SSL)

---

- Stateful firewalling and port-by-port filtering
- SSL or TLS to encrypt traffic
- Identity often only established after visitor decides to buy (credit card)
- The focus of most e-commerce security



# The big question

---

- So which will win?
  - Or is there a niche for both?