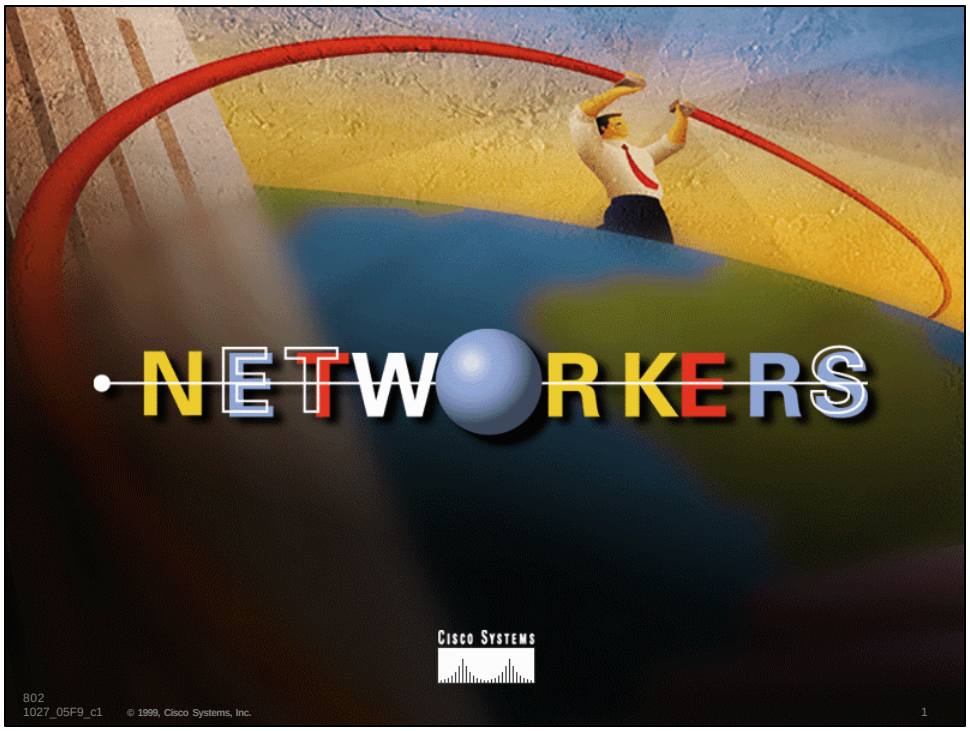
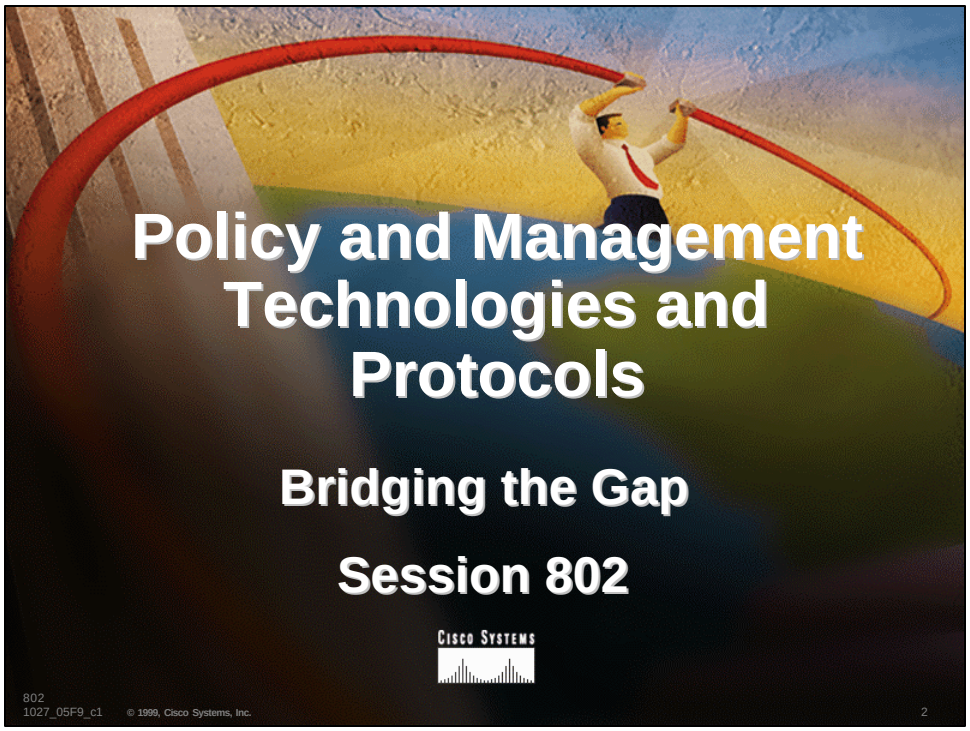




Outline of Talk

- What Is Policy?
- How Does Policy Map to Reality?
- How Do Policy Standards Fit Together to Make a Policy Framework?

What Is Policy?

- A goal statement

  Allow HTTP traffic from engineering to the company server

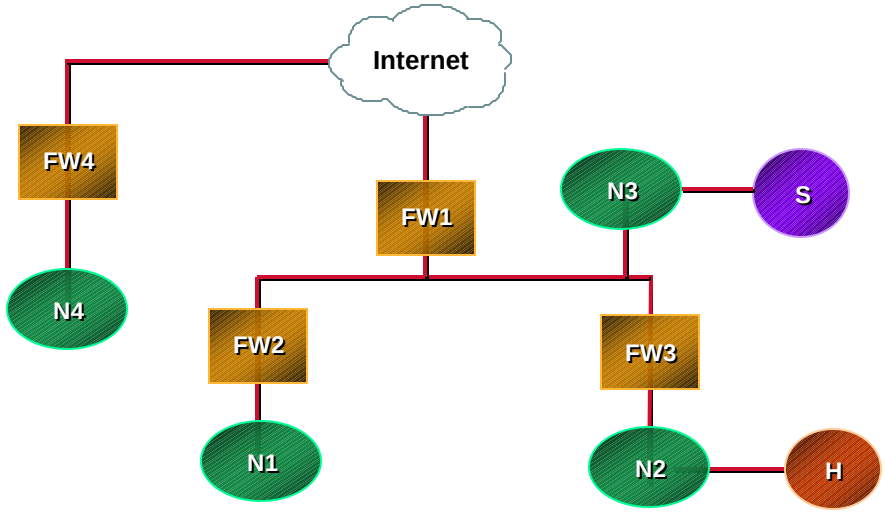
- Configuration specifies the mechanism

  On this firewall allow HTTP traffic on interface 3 from 192.168.45.0 to 128.100.15.56

Policy Targets

- Security
- Quality of service
- Routing

Example Administrative Domain



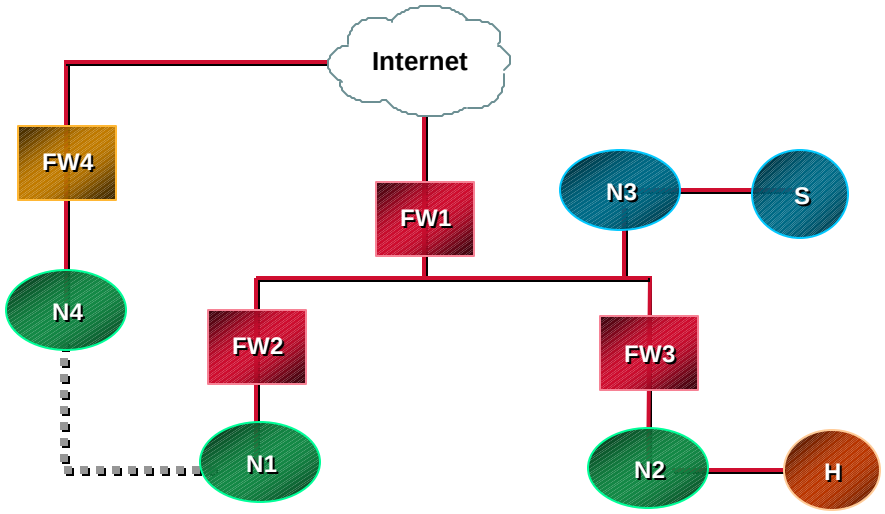
Policy Translation Steps

- Define topology
- Define policy rules
- Compile policy rules to specific device configurations

Topology

- Network relationships
- Enforcement points
  - Where are they?
  - What are they capable of?
  - What specific configuration is needed?

Domains of Constant Policy



802
1027_05F9_c1 © 1999, Cisco Systems, Inc. www.cisco.com 9

Policy Rules

- **Conditions**
  - Packet header
  - External conditions
  - User
- **Actions**
  - Filter rules
  - Encryption requirements
  - Quality of service requirements

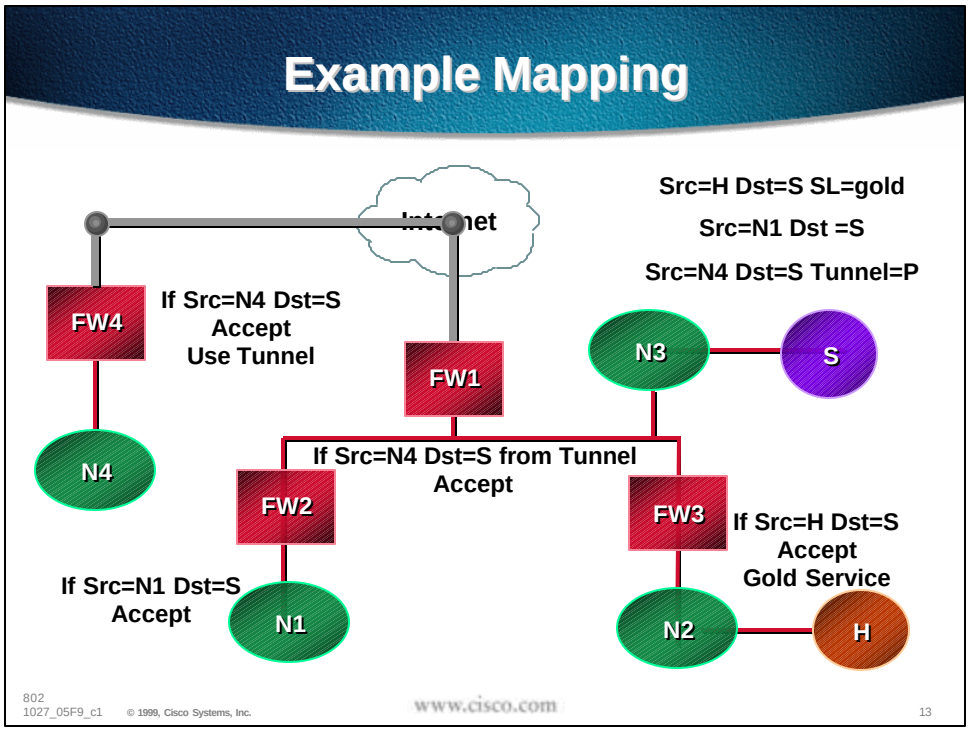
802
1027_05F9_c1 © 1999, Cisco Systems, Inc. www.cisco.com 10

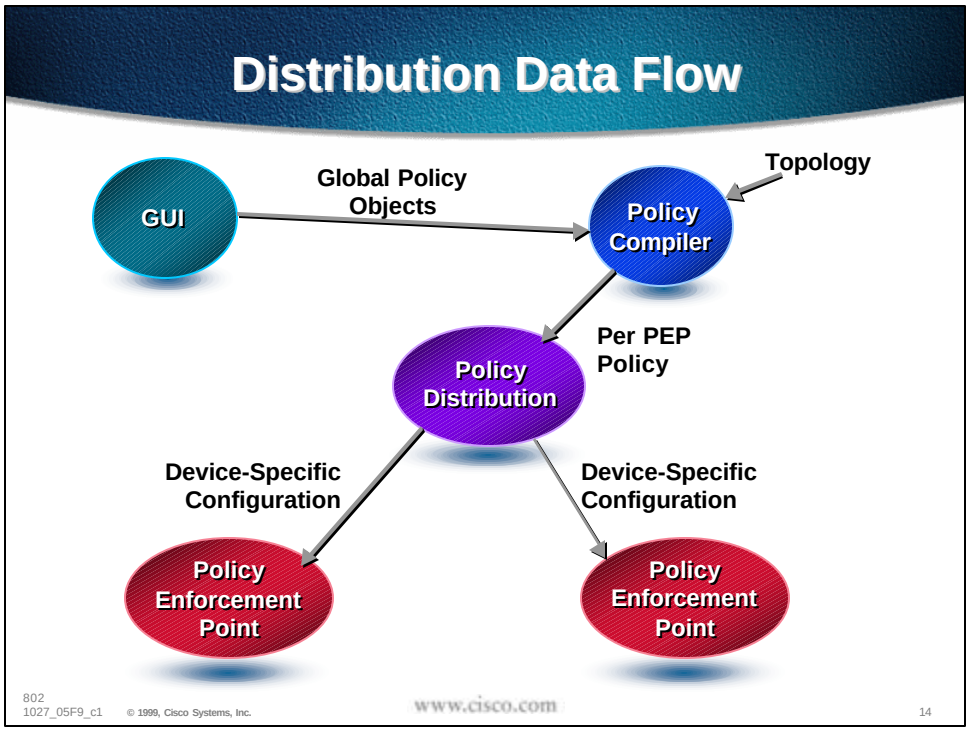
Example Policy

```
If service is HTTP
    if destination is S
      if source is H
            service level = Premium
            permit
      else if source is N1 or N4
            permit
      if source is N4
            use tunnel
```


Compilation Phase

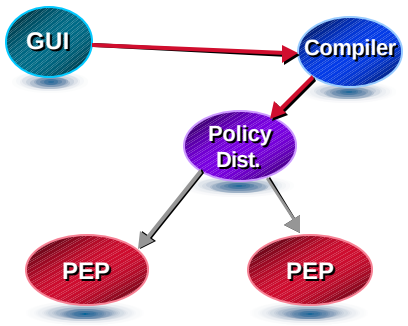
- Prune global policy for each enforcement point
- Resolve conflicting rules
  - Tunneling and filtering
  - QOS and tunneling
  - Resource limitations





Transport Technologies

- GUI to policy compiler
  - Message passing
  - Database
  - Directory



Policy Schema Standards

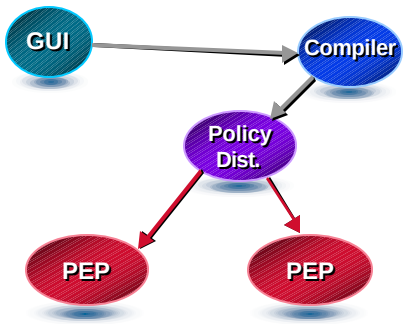
- Goal
  - Interoperability between policy tools
  - Identify core policy enforcement issues
- Many different working groups
  - IPSEC schema (IPSEC WG)
  - QOS schema (policy WG)
  - Policy languages
    - SPSL (IPSEC WG)

New Policy WG

- Targeting QOS domain
- Generated core schema draft
  - Specific domains inherit from the core classes
  - Schemas assume LDAP
  - Cooperation with the DEN schema

Transport Technologies

- Policy compiler to enforcement points
  - Telnet and command line interface
  - TFTP
  - SNMP
  - COPS

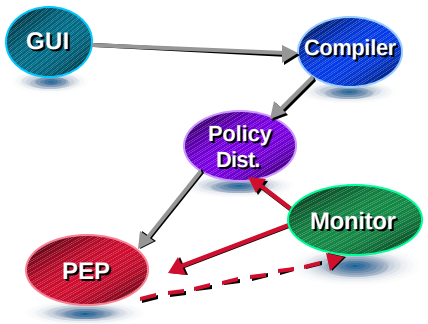


Common Open Policy Service

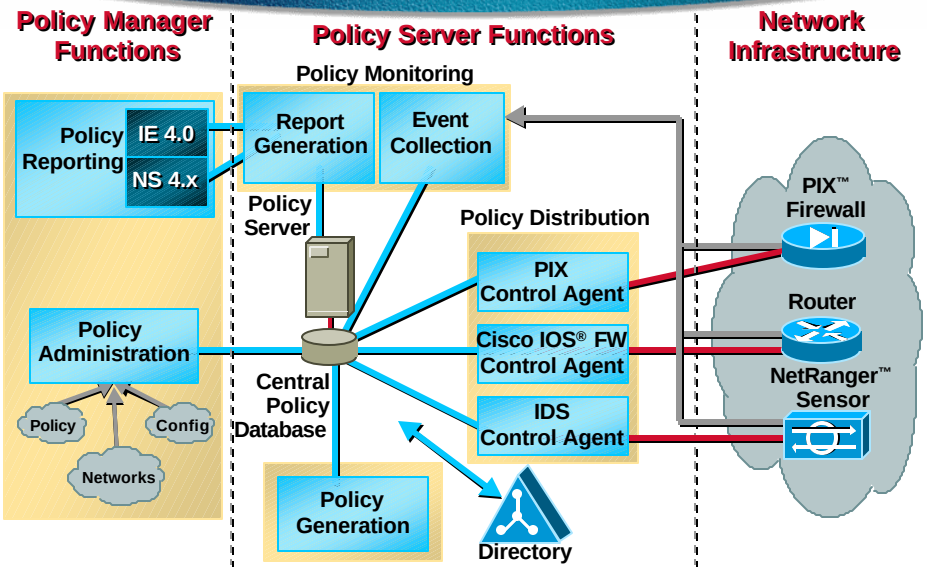
- A policy protocol designed for QoS
  - Close to RFC
- Single protocol, two uses
  - RSVP queries: draft-ieft-rap-cops-06.txt
  - Policy provisioning: draft-sgai-cops-provisioning.txt

System Feedback

- Variety of sources
  - syslog
  - SNMP traps
  - sniffing
- Adjust evaluation of policy



Security Manager Architecture



802
1027_05F9_c1 © 1999, Cisco Systems, Inc. www.cisco.com 21

The Bottom Line

- **Policy management can help create understandable, secure, maintainable network systems**

802
1027_05F9_c1 © 1999, Cisco Systems, Inc. www.cisco.com 22

Translation Is Key

- Generate consistent configurations from global rules
- Perform consistency checks between requested rules and generated hardware
- Use emerging policy mechanism standards

For More Information

- Cisco products
  - Cisco Security Manager
    - Session 1112
  - QoS Policy Manager
    - Session 807
- IETF standards
  - http://www.ietf.org
  - Policy Schemas
  - COPS drafts