

*TOMORROW starts here.*



Cisco *live!*

# Policy Driven Data Centre Design

BRKAPP-9001

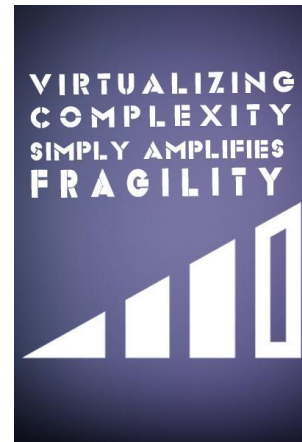
Joe Onisick

Technical Marketing Engineer INSBU

# Agenda

- What is policy?
- Policy and the network
- Defining application logic through policy
- Automating infrastructure through policy
- Advantages of policy driven data centre design

“Virtualising complexity simply **amplifies fragility.**”



Joe Onisick  
Cisco Systems



“Only a real jerk would quote themselves during a presentation.”

Joe Onisick  
Cisco Systems





What is Policy?

# What is Policy?

## Policy in Broad Terms



### pol-i-cy

A course or **principle of action** adopted or proposed by a government, party, **business**, or **individual**.

Synonyms: plans, strategy, stratagem, approach, **code**, **system**, guidelines, theory...

# What is Policy?

## Policy and Intentions



No smoking is the policy. It is the intention. It is up to individuals (objects) to follow that intention.



Enforcement and auditing of the policy is separate from policy definition.



Actions can be taking for violations of policy (faults.)

Policy can be thought of a set of rules defining desired state.



# What is Policy?

## Policy and Desired State



A no parking sign is policy used to define the desired state of a section of road. The desire is, road free from parked cars.



Desired state does not, in and of itself, enforce state. Drivers (objects) are expected to implement and adhere to desired state.



Auditing can be performed against both desired and current state.

Desired state is the intended condition of an object which can be expressed via policy.

# What is Policy?

Desired vs. Current State

Desired State



Expression of  
intent based on  
policy



Current State



Actual  
implementation  
of desired state



Non-Compliance  
Alert

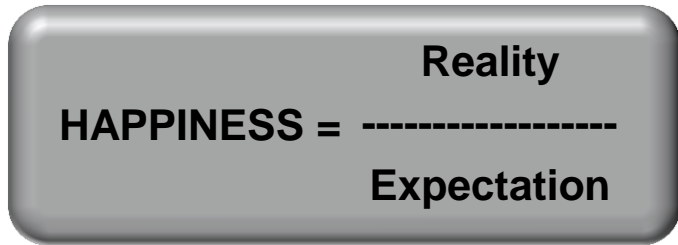


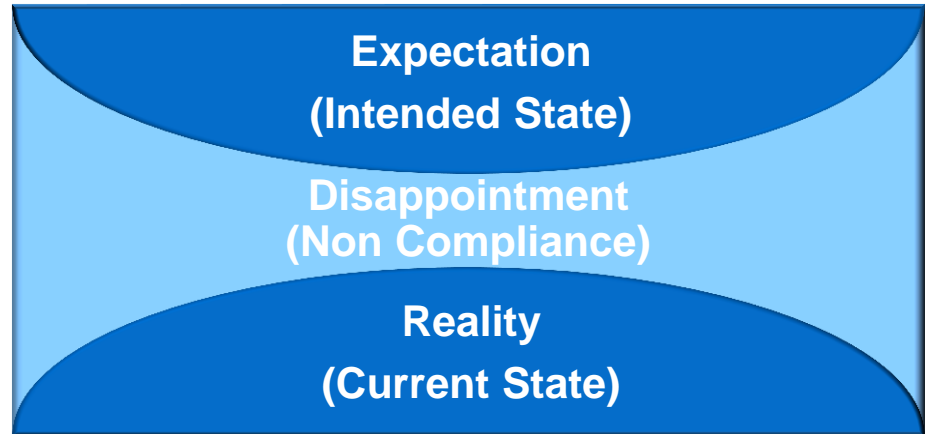
Report of  
current state  
exceptions

Mismatches between desired and current state generates faults or exceptions.

# What is Policy?

The Goal of State


$$\text{HAPPINESS} = \frac{\text{Reality}}{\text{Expectation}}$$



The goal is to minimize the gap between expectation and reality.



# Policy and the Network

# Policy and the Network

What is network policy?

Basic Network Policy



SLA Policy



L4-7 Services



Network policy involves all of the rules required for end-to-end application connectivity.

# Policy and the Network

## Traffic Identification



5 Tuple Match

**ORACLE**<sup>®</sup>

Microsoft<sup>®</sup>  
**Exchange**

Microsoft<sup>®</sup>  
**SharePoint**<sup>®</sup>

**SAP**<sup>®</sup>

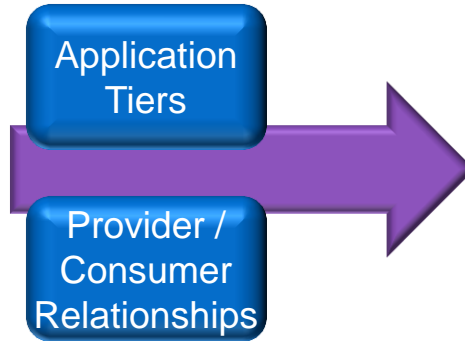
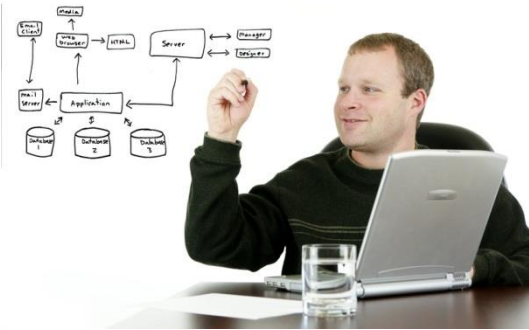
**Java**

Applications, users, groups, etc. must be identified based on network header information.

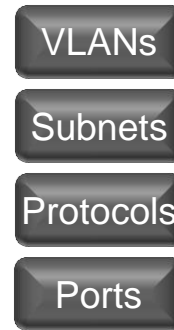
# Policy and the Network

## Application Language Barriers

### Developers



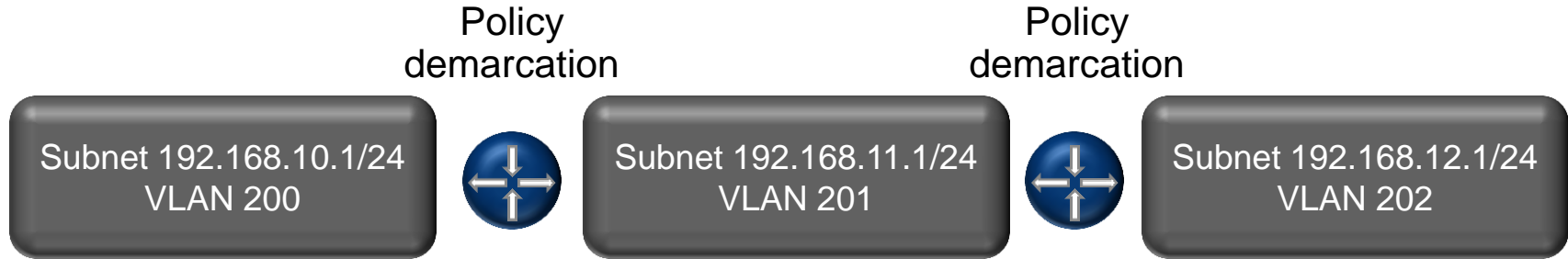
### Infrastructure Teams



Developer and infrastructure teams must translate between disparate languages.

# Policy and the Network

## Policy Definition on Today's Networks

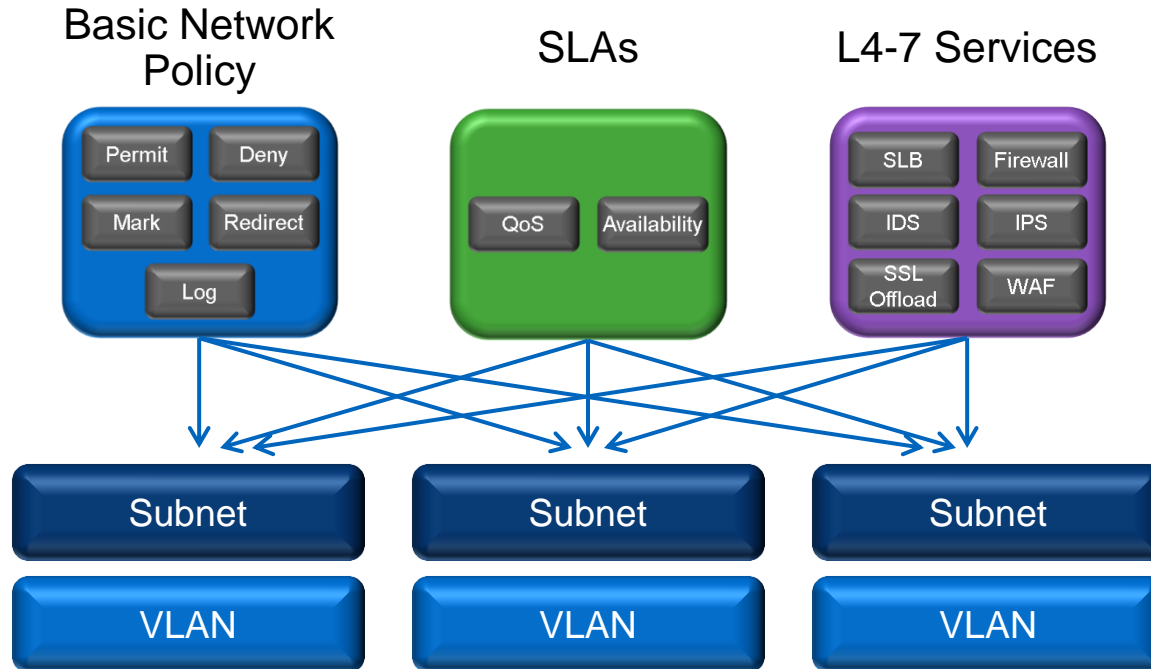


Construct	Intended Purpose	Current Usage
VLAN	Flood Domain	Flood Domain Subnet demark
Subnet	Forwarding address	Forwarding address Policy boundary Security identifier Application identifier



# Policy and the Network

## Overloaded Network Constructs



Network constructs are overloaded with unintended functionality.

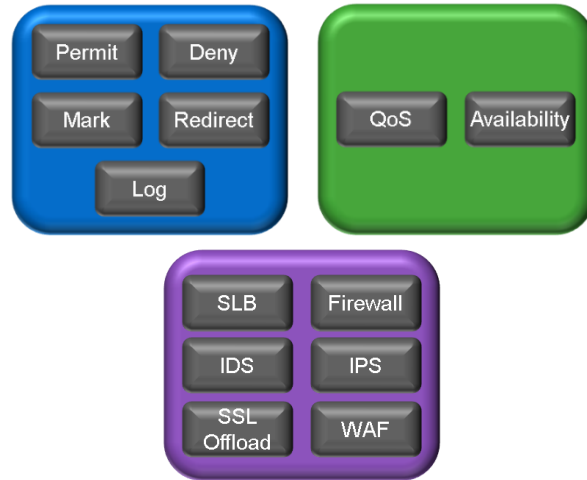
# Policy and the Network

## Simple Changes Cause Big Implications

10.10.10.201



Intended IP change



Unintended policy  
change requirements

Changes at any layer of the stack have effects throughout the stack.



## Defining Application Logic Through Policy

# Defining Application Logic Through Policy

Warning!



## WARNING

Forget everything you know  
about networking for the  
remainder of this session



Believe!

“The moment you doubt whether you can fly, you cease for ever to be able to do it.”

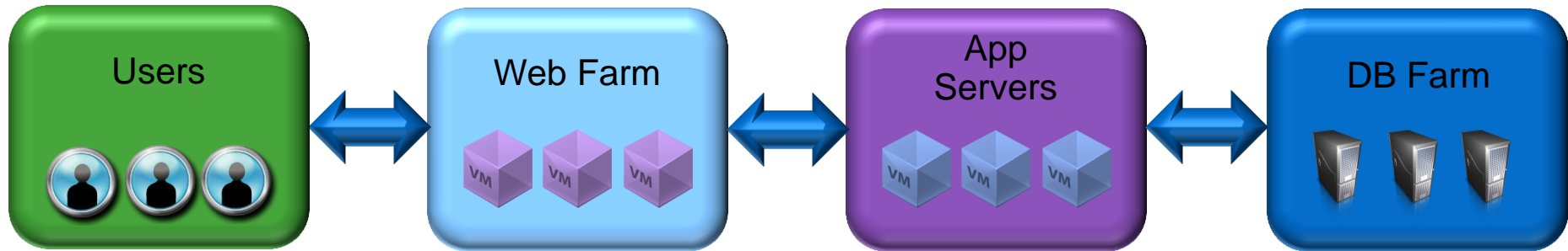
J.M. Barrie  
Peter Pan



# Defining Application Logic Through Policy

## Applications and Conversations

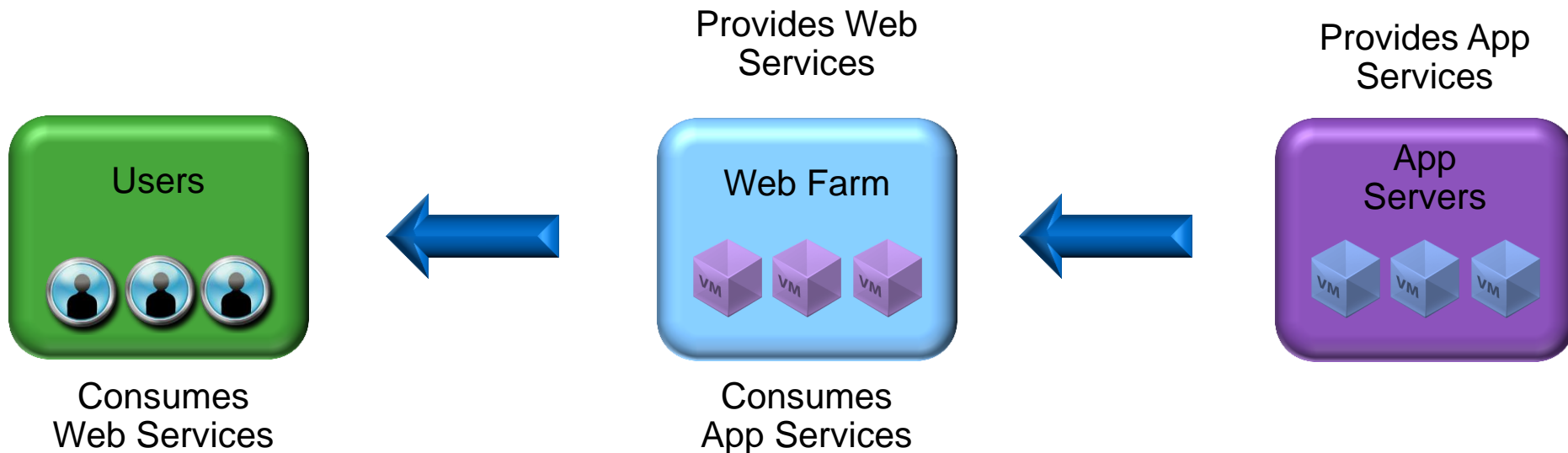
Application communication can be defined as who is allowed to talk to whom.



Communication between objects on the network can be thought of as one or two way conversations (monologue/dialogue.)

# Defining Application Logic Through Policy

## The Provider Consumer Relationship



Provider consumer relationships define application connectivity in application terms. All objects can provide, consume, or both.

# Defining Application Logic Through Policy

## Contracts for Policy



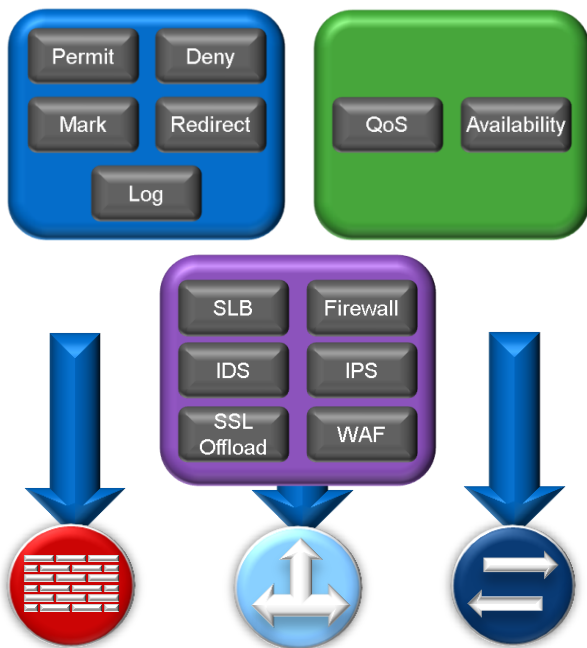
Contracts are used to define relationships.



# Defining Application Logic Through Policy

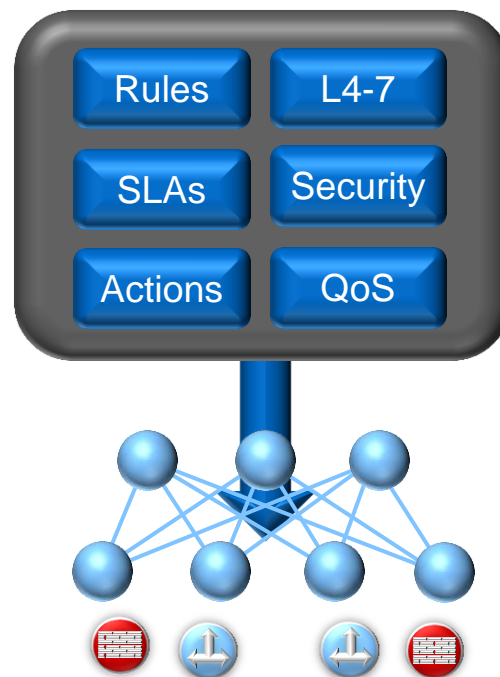
## Policy Definition

### Current Policy Definition



BRKAPP-9001

### Policy Based on Contracts



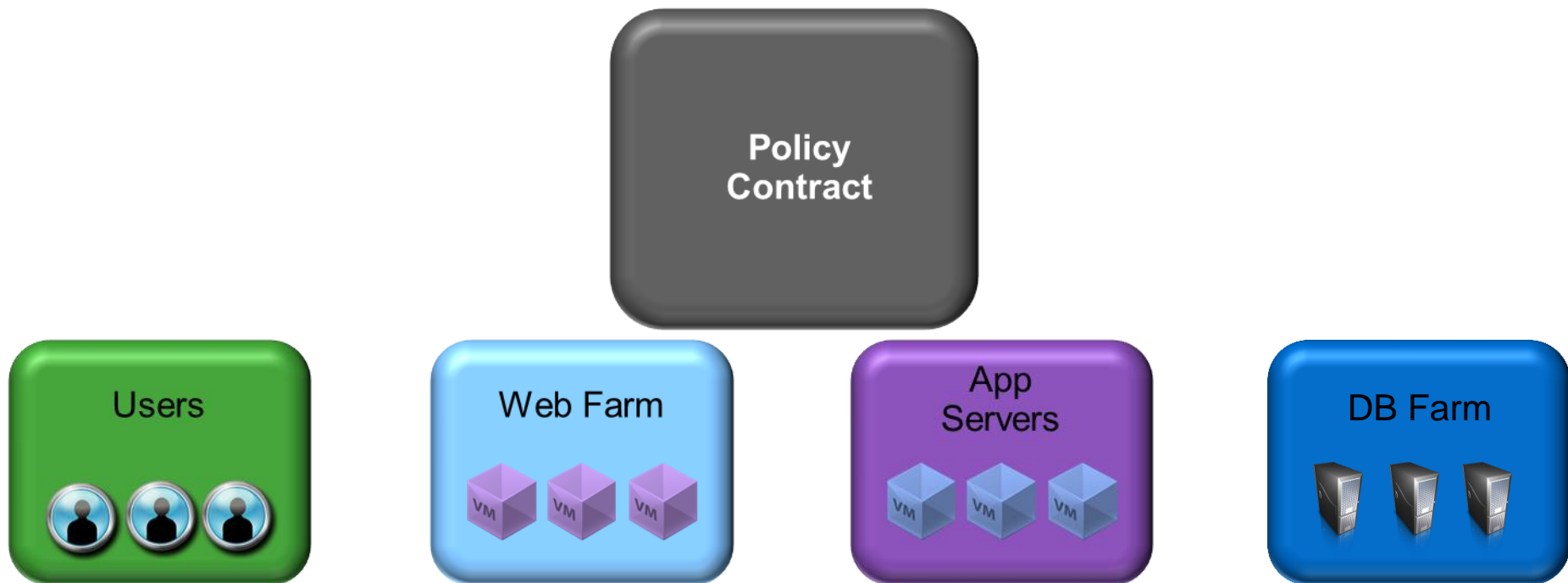
Cisco Public

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco *live!*

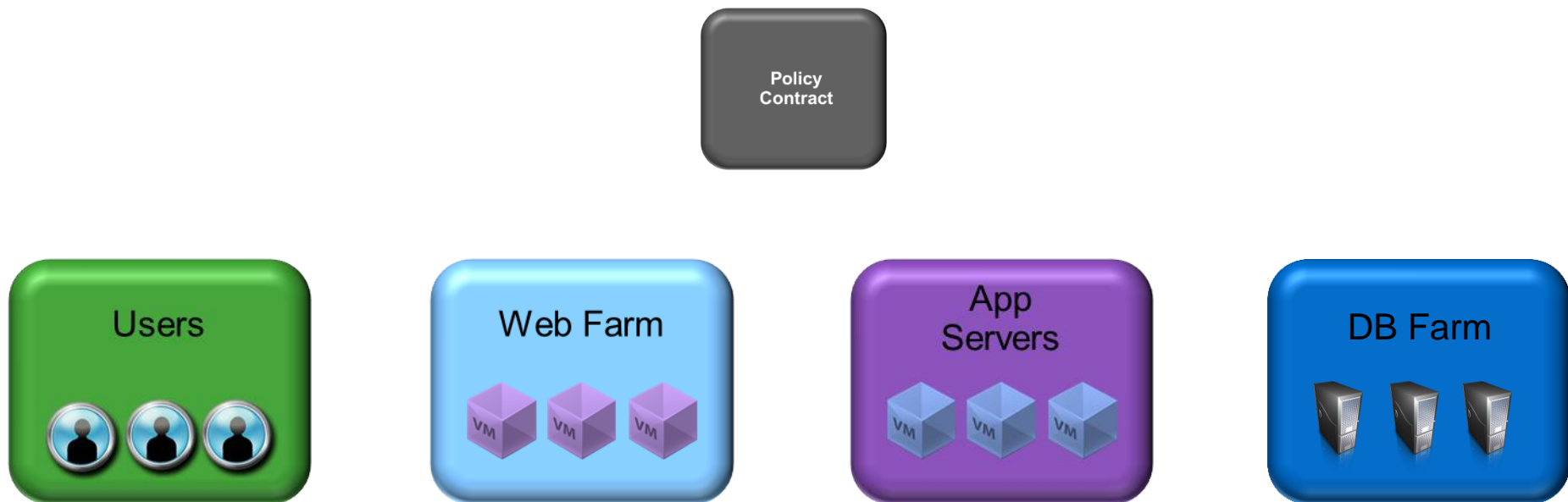
# Defining Application Logic Through Policy

## Defining Provider Consumer Relationships



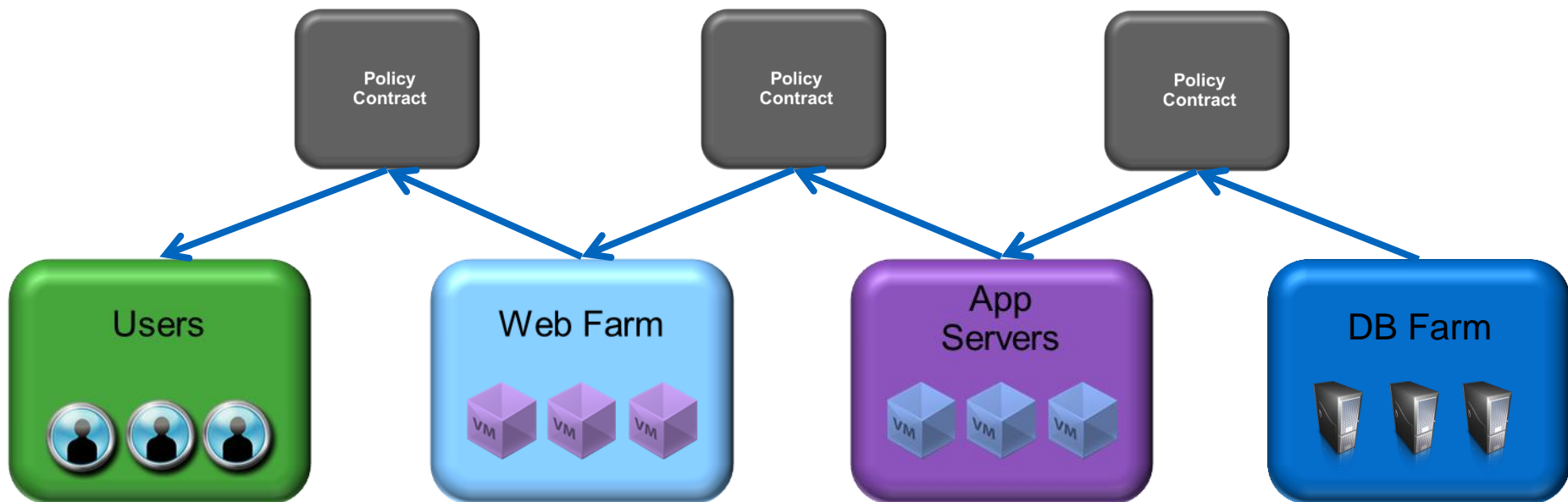
# Defining Application Logic Through Policy

## Defining Provider Consumer Relationships



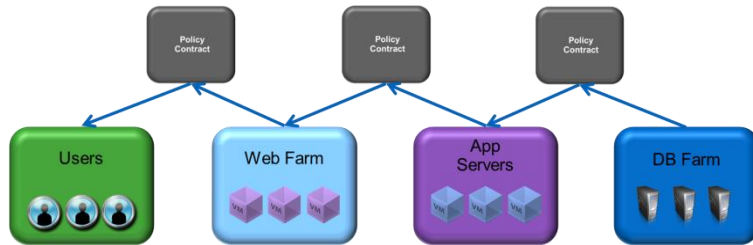
# Defining Application Logic Through Policy

## Defining Provider Consumer Relationships



# Defining Application Logic Through Policy

## Object Relationships



- Relationships between objects/groups are defined by providing or consuming contracts.
- Connectivity is 'turned on' by creating relationships.
- Objects/groups can provide, consume, or both.

Consumer provider relationships define which objects or groups can communicate and the policy requirements for that connectivity.

# Defining Application Logic Through Policy

Simple Changes Remain Simple

10.10.10.201



Intended IP change



Policy remains the same independent of end-point change

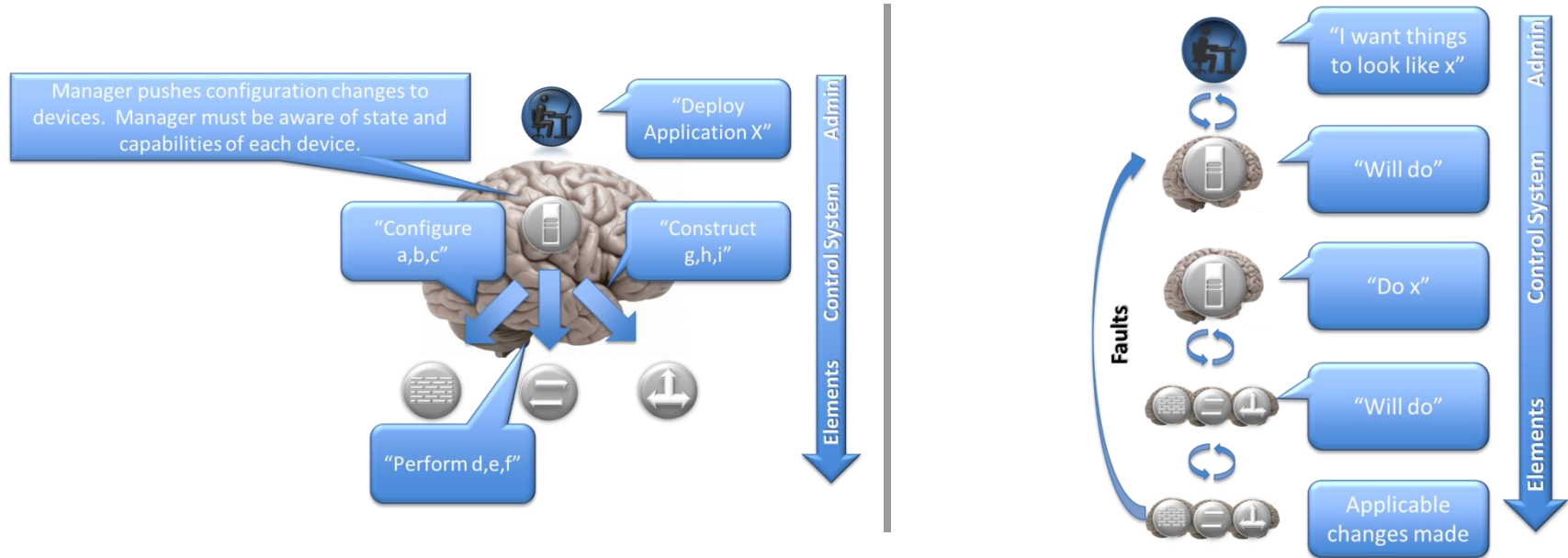
Changes at any layer of the stack are independent of one another.



## Defining and Instantiating Policy

# Defining and Instantiating Policy

## Intended State and Promise Theory



Promise theory relies on trust that a device will apply intended state and report non-compliance.



# Defining and Instantiating Policy

## Defining Infrastructure Policy

Policy can be defined in a reusable format. As a logical configuration of intended state.

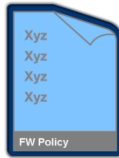


Policy can be used to define the configuration state of logical, virtual and physical elements.

Used broadly policy is a reusable format for defining the intended state of objects.

# Defining and Instantiating Policy

## Applying Policy to Infrastructure



Policies can be defined logically then applied to infrastructure repeatedly where applicable.

# Defining and Instantiating Policy

## Handling Non-Compliance



When objects are unable to apply intended state, non-compliance is reported back to the object issuing intended state.



# Automating Infrastructure Through Policy

# Automating Infrastructure Through Policy

## What is Automation?

**Automation** or *automatic control*, is the use of various control systems for operating equipment such as machinery, processes in factories, boilers and heat treating ovens, switching in telephone networks, steering and stabilisation of ships, aircraft and other applications with minimal or reduced human intervention... – Wikipedia.org



Avoid This!



Avoid This!



Automation can speed up processes, but also reduce risk of human error.

“To err is human, to apply that error to 1000 servers at once is DevOps.”

Unknown



# Automating Infrastructure Through Policy

## Using Policy for Automation



# Automating Infrastructure Through Policy

## Policy and Automation



Policy can be used to:

- Apply intended state configuration
- Apply intended state change
- Provide event based actions

Policy can be applied as a logical definition for automating configuration, state, and event handling.

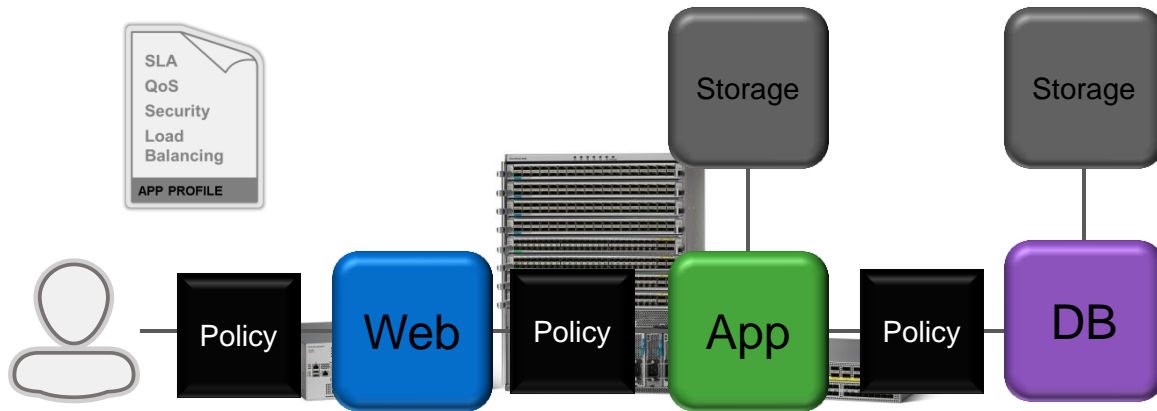




## Advantages of Policy Driven Data Centre Design

# Advantages of Policy Driven Data Centre Design

## Abstraction



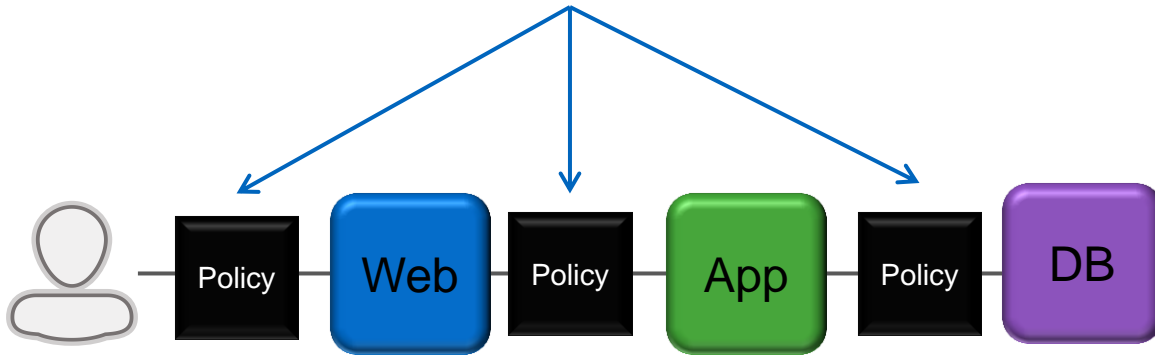
Policy abstracted as a logical definition of intended state.

Physical and virtual objects are responsible for applying state.

# Advantages of Policy Driven Data Centre Design

## Extensibility

Policy used to describe connectivity can be extended as requirements/capabilities change.



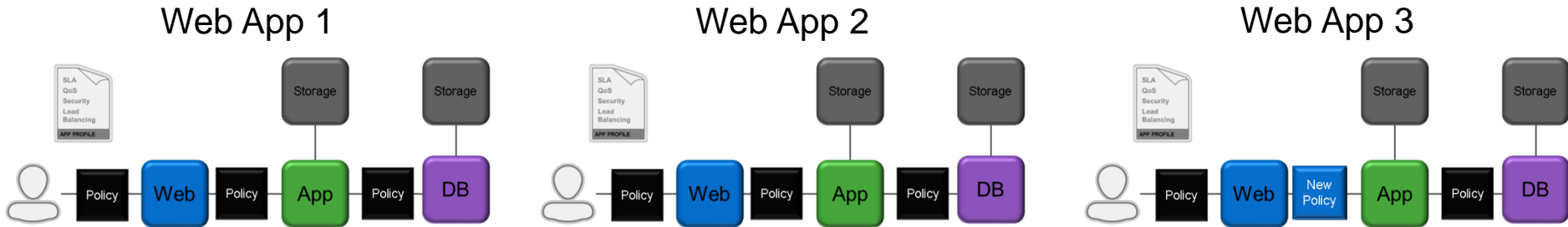
Policy used to describe configuration will be updated with HW/SW capability.



Logical policy objects provided a common toolset for defining the intended policy state of objects.

# Advantages of Policy Driven Data Centre Design

## Reuse



Policy definition can be reused at multiple levels.

“If you don’t like change, you’re going to like irrelevance even less.”

General Eric Shinseki  
United States Army



# Summary

- Policy is a broad term that can be used to describe intended state
- When intended state and current state do not match non-compliance alerts are generated.
- The goal is to match intended state as closely as possible to actual state while allowing agility and scale.
- Policy on the network encompasses many configurations and touch-points.
- Contracts can be used to centralise policy for ease of use and reuse.
- Policy can be used to automate infrastructure, and provide consistent deployments.



Q & A

# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site [www.ciscoliveaustralia.com/mobile](http://www.ciscoliveaustralia.com/mobile)
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm



## Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.

[www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)





**CISCO**™