

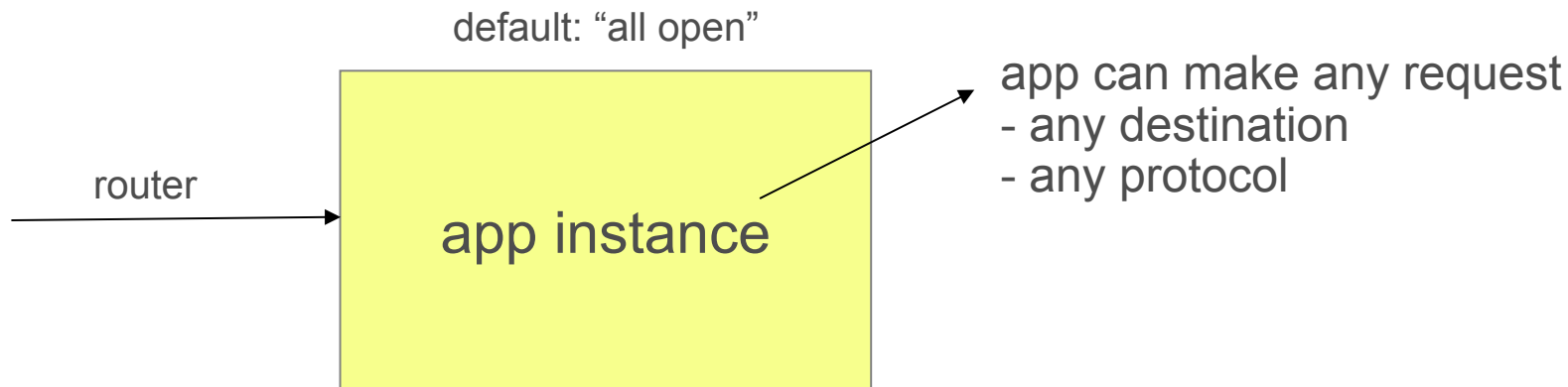
Application Security Groups

Topics

- **Application Security Group overview**
- Application Security Group of CLI commands

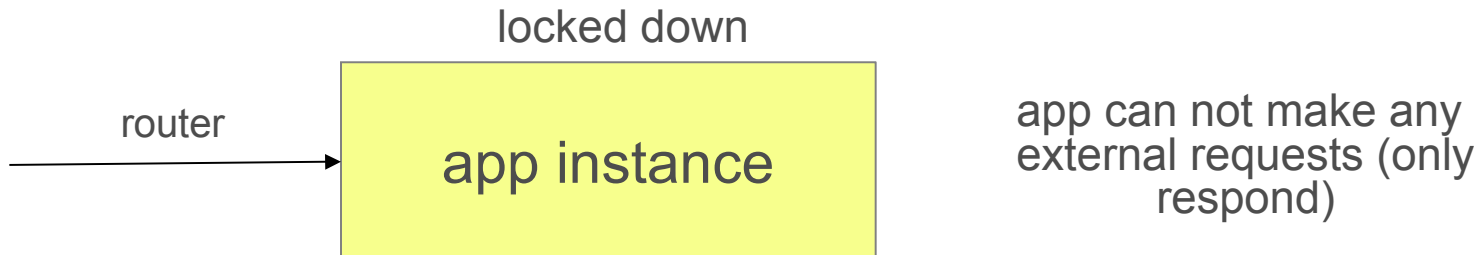
Application Security Groups- Default

- Application Security Groups enable application containers to be locked down to only necessary outbound connections
- By default, outbound traffic from application containers is not locked down



Application Security Groups- Locked Down

- Can set rules to enable access to only certain IP addresses and/or protocols
 - Acts as a virtual firewall
 - Especially useful for highly regulated industries (financial services, government, healthcare, etc.)
- The application containers are locked down by operators and the security rules are viewable by developers



Application Security Group Rules

- Enable specific egress (outgoing) traffic
 - Whitelist (allow) only
 - No support for deny
- Rules specify:
 - Protocol: TCP, UDP, ICMP
 - Open port/port range
 - Destination IP address or CIDR block
- Rules are specified in a JSON file

Example JSON File

- Only the protocols, IP address and ports listed are allowed
 - TCP to *ip-foo:3306*
 - TCP in IP range *some-ip* to *another-ip* on port 55882

```
[  
  { "protocol": "tcp",  
    "destination": "<ip-foo>",  
    "ports": "3306" },  
  
  { "protocol": "tcp",  
    "destination": "<some-ip>-<another-ip>",  
    "ports": "55882" }  
]
```

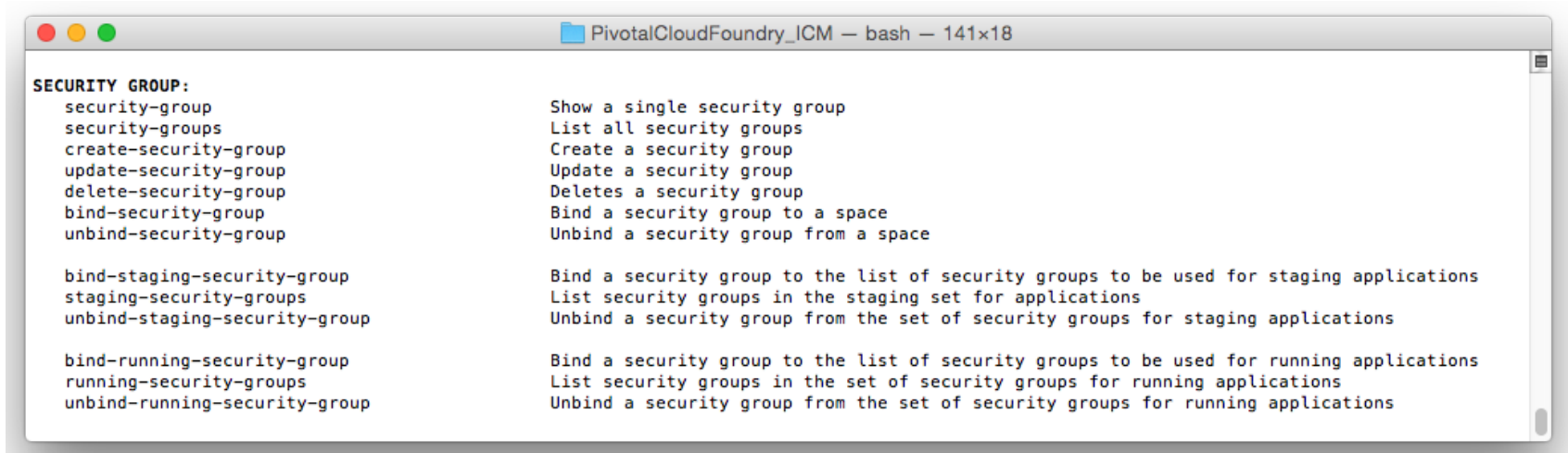
Application Security Group Scope

- Can be deployment wide (any space) or space-specific
- Can apply to staging (push) or runtime
 - Staging may allow more outbound traffic for things like downloading external files/artifacts

Topics

- Application Security Group overview
- **Application Security Group cf CLI commands**

Application Security Group CLI Commands



A terminal window titled "PivotalCloudFoundry_ICM — bash — 141x18" displays a list of CLI commands for Application Security Groups. The commands are organized into three sections: "SECURITY GROUP:", "staging-security-groups", and "running-security-groups". Each command is followed by a brief description of its function.

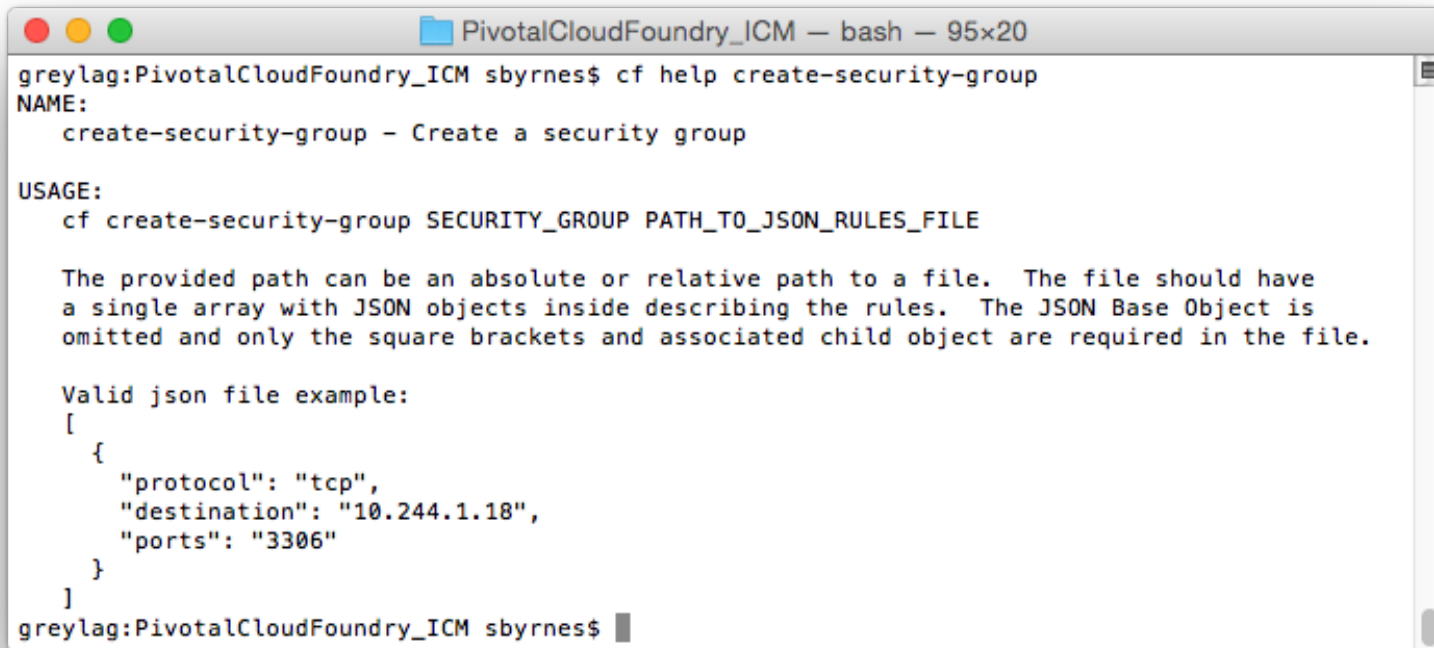
```
PivotalCloudFoundry_ICM — bash — 141x18

SECURITY GROUP:
security-group          Show a single security group
security-groups         List all security groups
create-security-group   Create a security group
update-security-group   Update a security group
delete-security-group   Deletes a security group
bind-security-group     Bind a security group to a space
unbind-security-group   Unbind a security group from a space

bind-staging-security-group Bind a security group to the list of security groups to be used for staging applications
staging-security-groups   List security groups in the staging set for applications
unbind-staging-security-group Unbind a security group from the set of security groups for staging applications

bind-running-security-group Bind a security group to the list of security groups to be used for running applications
running-security-groups   List security groups in the set of security groups for running applications
unbind-running-security-group Unbind a security group from the set of security groups for running applications
```

Creating an Application Security Group



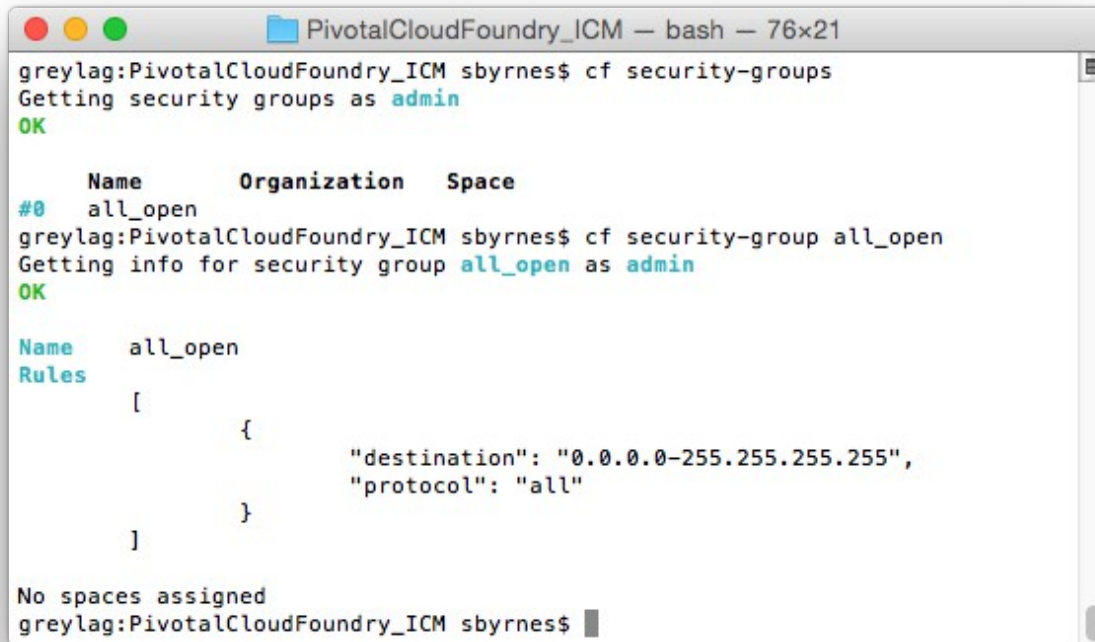
```
PivotalCloudFoundry_ICM — bash — 95x20
greylag:PivotalCloudFoundry_ICM sbyrnes$ cf help create-security-group
NAME:
  create-security-group - Create a security group

USAGE:
  cf create-security-group SECURITY_GROUP PATH_TO_JSON_RULES_FILE

The provided path can be an absolute or relative path to a file. The file should have
a single array with JSON objects inside describing the rules. The JSON Base Object is
omitted and only the square brackets and associated child object are required in the file.

Valid json file example:
[
  {
    "protocol": "tcp",
    "destination": "10.244.1.18",
    "ports": "3306"
  }
]
greylag:PivotalCloudFoundry_ICM sbyrnes$
```

Default Installation- No Container Lockdown

A terminal window titled "PivotalCloudFoundry_ICM — bash — 76x21" showing the configuration of a security group in Cloud Foundry. The user runs 'cf security-groups' and 'cf security-group all_open'. The output shows a table with columns Name, Organization, and Space. The 'all_open' group is listed with Organization 'sbyrnes' and Space 'all_open'. The rules for 'all_open' are shown as a JSON array with a single rule allowing all traffic to all destinations.

```
greylag:PivotalCloudFoundry_ICM sbyrnes$ cf security-groups
Getting security groups as admin
OK

      Name      Organization  Space
#0  all_open
greylag:PivotalCloudFoundry_ICM sbyrnes$ cf security-group all_open
Getting info for security group all_open as admin
OK

Name      all_open
Rules
  [
    {
      "destination": "0.0.0.0-255.255.255.255",
      "protocol": "all"
    }
  ]

No spaces assigned
greylag:PivotalCloudFoundry_ICM sbyrnes$
```

Binding an Application Security Group

- Deployment-wide
 - bind-staging-security-group
 - bind-running-security-group
- Space-specific
 - bind-security-group
- You can bind multiple Application Security Groups
 - Any rule that allows the outbound traffic sets the request to *allow*

Topics

- Application Security Group overview
- Application Security Group of CLI commands

Lab

Create and apply Application Security Groups