

# 알고섹을 이용한 클라우드 보안 정책관리

ALGOSEC SECURITY MANAGEMENT  
FOR HYBRID CLOUD

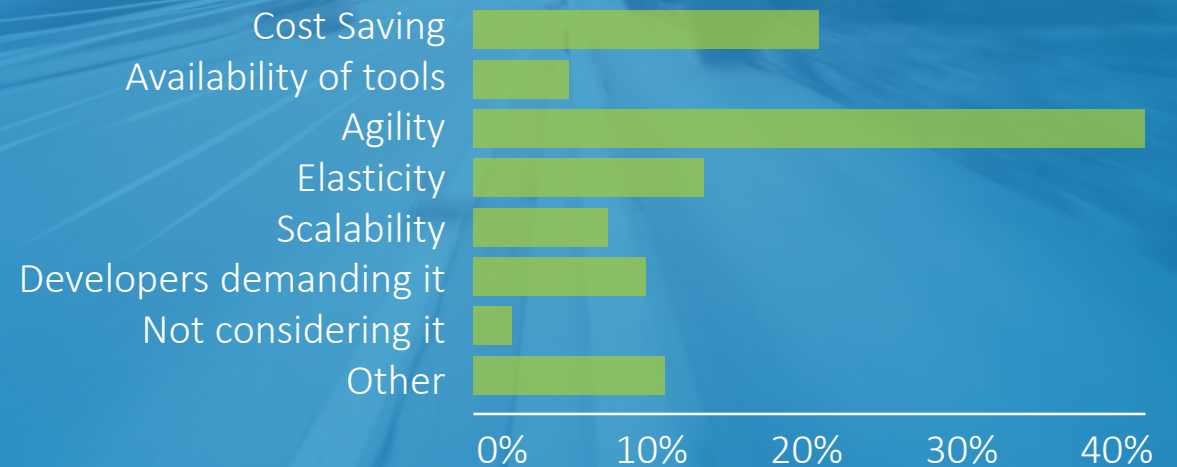
MANAGE SECURITY  
AT THE SPEED OF BUSINESS



# In the cloud, **agility** and **automation** are more important than ever

What is your PRIMARY motivation for deploying Public Cloud IaaS

**Gartner**<sup>®</sup>



Security Controls are Different

Security fundamentals remain the same

“Through 2019, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities.”

**Gartner**<sup>®</sup>

# NOT EVERYBODY MIGRATES TO THE CLOUD

- We know our customer's **vision** – *migration*
- It involves our cutting edge features
  - Application (Auto) Discovery
  - Seamless submission of FireFlow change requests
  - End to end automation including ActiveChange
  - Accurate analysis of tens of Security Groups, NACLs
  - Etc.
- A BIG project that requires heavy resources and careful planning



*But wait, there is another use case...*

# THE OVERWHELMED SECURITY TEAMS

- Professionals at managing on premise devices
- Fluent in their firewalls' policies
- Understand their security posture and policy

*And one day their manager tells them about the cloud...*

- How to make *first contact* with these unmanaged cloud servers?
- This is what they need *NOW*

# CLOUD SECURITY – THE PRAGMATIC START

- Change monitoring – very valuable!
  - Alerting
  - Reviewing

Step 1

- Visibility into running servers
- Detailed change reporting
- Policy visibility
- Risk and compliance reports
- Troubleshooting (Traffic Simulation Queries)

Step 2

# ALGOSEC SUPPORT FOR THE SIMPLE STORY

## Amazon Web Services (AWS) and VMWare NSX

- Visibility into running servers
- Full policy visibility
  - 6.9 – Security Groups and Distributed Firewalls
  - 6.10 – Network ACLs (NACLs)
- Detailed change monitoring
- Troubleshooting capabilities
- Change management support

Step 2

Step 1

## Microsoft Azure (6.10)

- Change monitoring

# AWS SUPPORT

The screenshot displays the Firewall Analyzer interface. At the top, it shows '5 changes' and 'instance\_11'. The main area features a network diagram with nodes: 'Rose\_checkpoint' (IP: 192.168.6.0/24), 'Poppy\_juniper' (IP: 10.176.50.160/29), and 'C18' (IP: 10.176.50.166). A red arrow points to the 'C18' node. A sidebar on the left lists 'Devices in Path (6)', categorized into 'BLOCKING (4)' (Rose\_checkpoint, Rose\_DR, Poppy\_juniper, SequoiaAWS\_US\_west\_coast) and 'ALLOWING (2)' (DC\_42, DC\_82). At the bottom, a rule table is visible with the following entries:

|  | Direction | Source           | Destination | Protocol | Port | Action |
|--|-----------|------------------|-------------|----------|------|--------|
|  | Inbound   | 84.95.251.227/32 | Host        | tcp      | 389  | ALLOW  |



Analyze from a file

Monitoring

- Cisco ACE
- Cisco Application Centric In
- DELL SonicWALL
- F5 BigIP
- H3C
- Juniper - Secure Access (SS
- Juniper Routers (non-M/E)
- Linux netfilter - iptables
- Microsoft Azure
- SECULME

**Access Information**

Type: M

Supported Capabilities: R

Name: (?)

Subscription ID: (?)

Tenant ID: (?)

Client ID: (?)

Key: (?)

**Raw Configuration**

Jul 0, 2016 | 12:36:37 PM

```
@@@ -209,28 +209,25 @@@
```

```
    "0.0.0.0/0"
```

```
  ],
```

```
},
```

```
{
```

```
  "ipProtocol": "tcp",
```

```
  "fromPort": 22,
```

```
  "toPort": 22,
```

```
  "ipRanges": [
```

```
    >
```

```
    "0.0.0.0/0",
```

```
    "1.0.0.0/24",
```

```
    "1.2.3.4/32"
```

```
  ],
```

```
  "0.0.0.0/0"
```

```
},
```

```
{
```

# BUSINESS-DRIVEN SECURITY POLICY MANAGEMENT FOR HYBRID CLOUD ENVIRONMENTS

## Application Migration to the Cloud

- Application auto-discovery and connectivity requirements mapping
- Automatic translation from firewall rules to cloud security controls
- End to end automation of new security policy creation

## Unified Security Policy Management across the Hybrid Environment

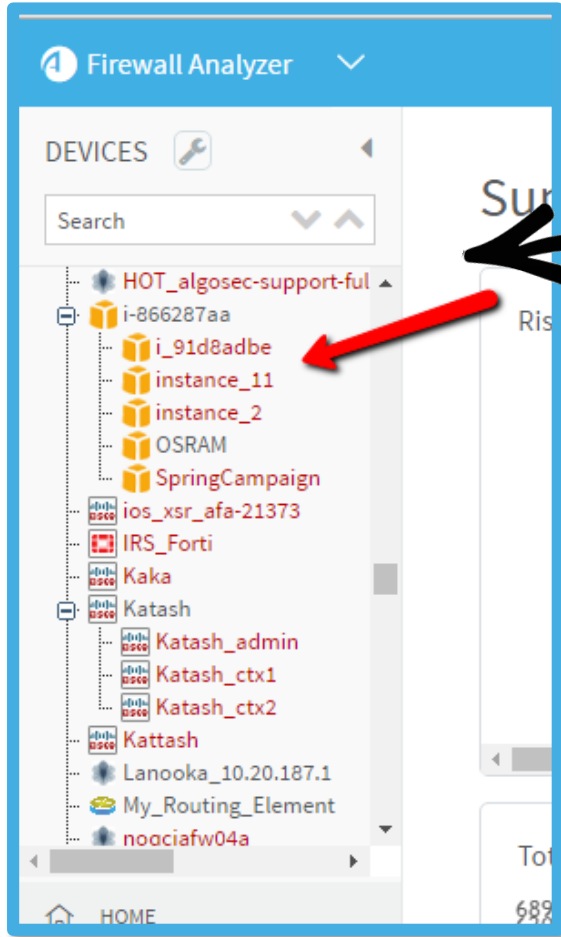
- Single pane of glass for firewall rules and cloud security controls
- Security policy visibility, monitoring and alerting
- Risk and compliance reports
- Troubleshooting and traffic simulation

Supported platforms:

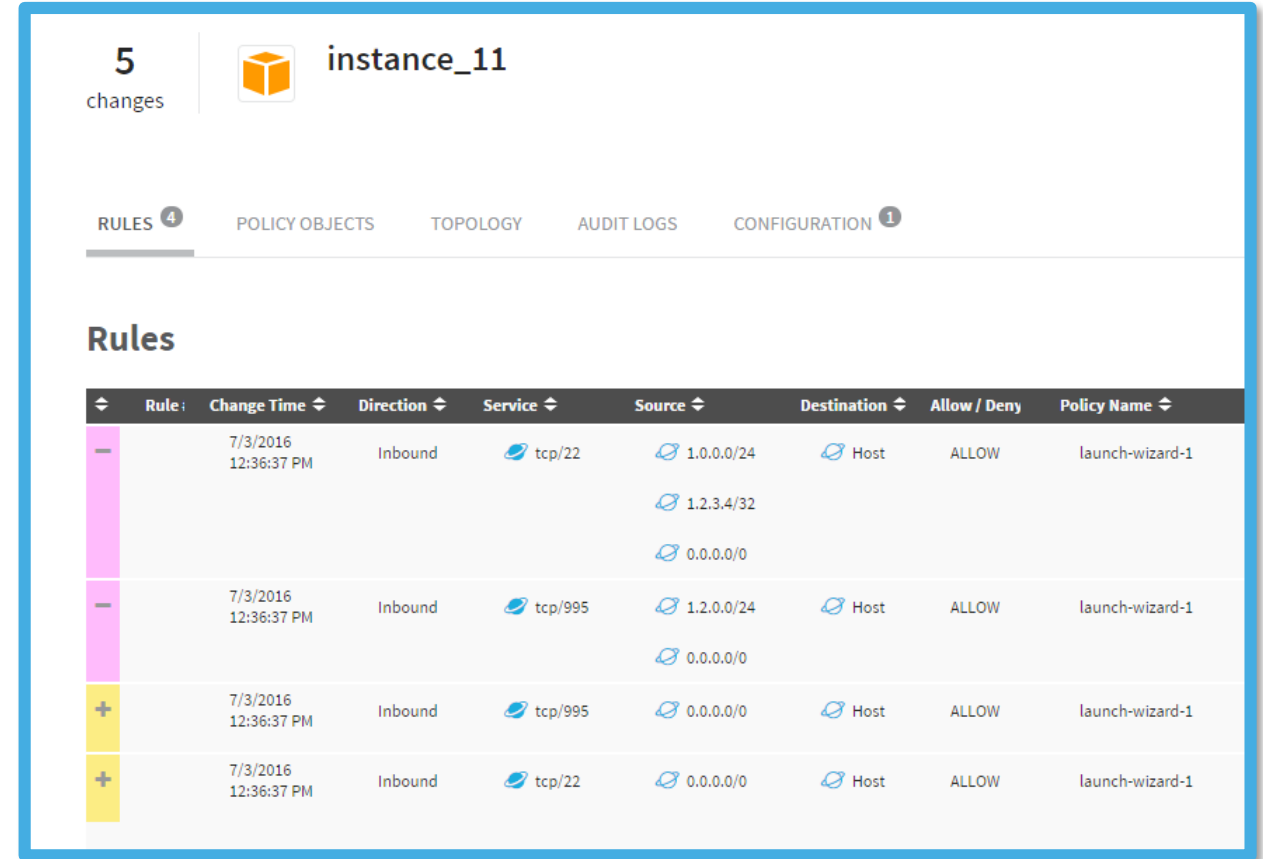


Microsoft Azure

# HYBRID CLOUD SECURITY POLICY MANAGEMENT

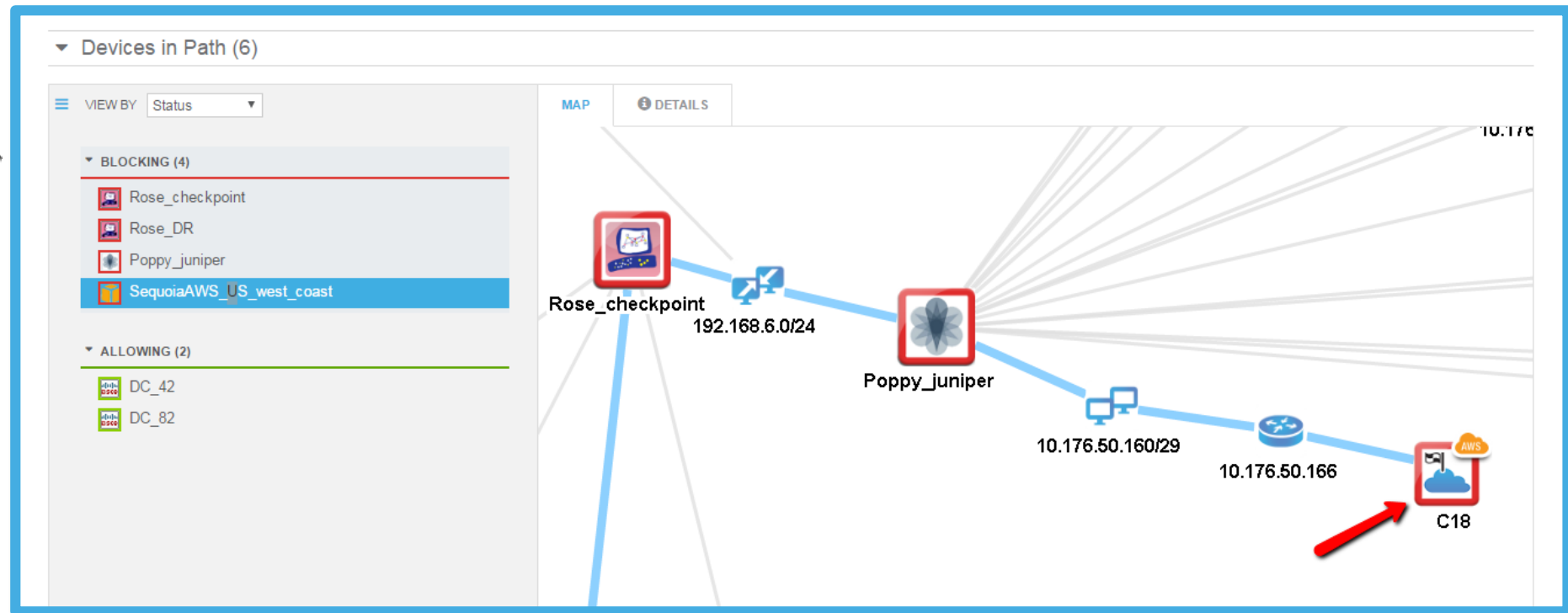


Visibility into running instances and their security controls



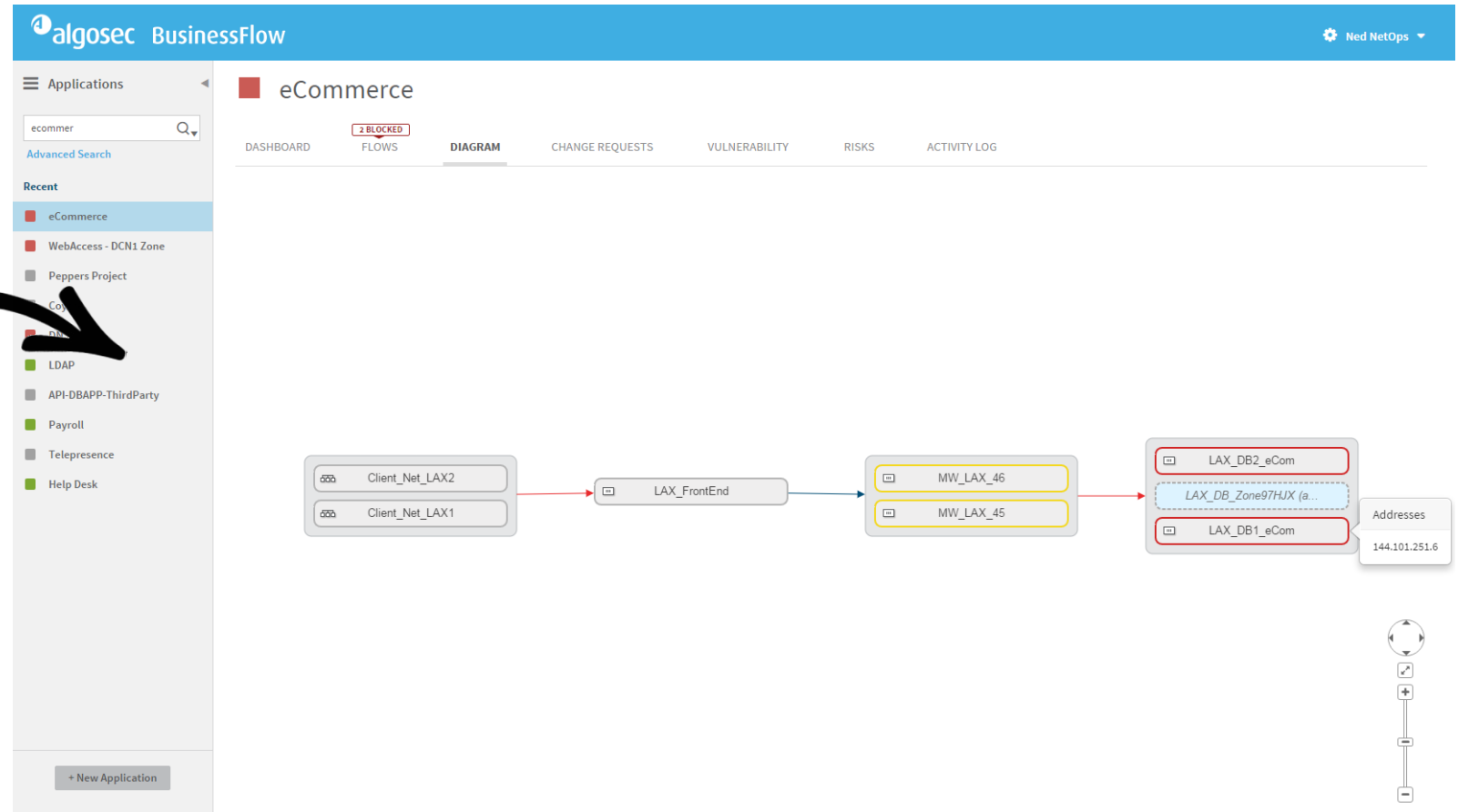
# HYBRID CLOUD SECURITY POLICY MANAGEMENT

Traffic simulation queries across the hybrid environment



# APPLICATION MIGRATION

Auto-discover applications and their connectivity requirements with zero prior knowledge



# APPLICATION MIGRATION

Create projects to migrate specific server(s) or entire applications



The screenshot shows a web form titled "New Server Migration Project". It includes a "Project Name" field with the text "Moving Time Clock Server from LAX to AWS", a "Project Description" text area, and an "Add Task" button with a sub-label "Add tasks from file". Below this is a table with three columns: "Existing Server", "New Server", and "Comment". The "Existing Server" column contains the IP address "64.46.192.1 (LAX time clock server)" with a "Network Object Lookup" link below it. The "New Server" column contains "Amazon cloud time clock server" with a "Create or Lookup Network Object" link below it. The "Comment" column is currently empty.

# APPLICATION MIGRATION

AlgoSec discovers affected applications and computes required changes to firewall rules and cloud security groups

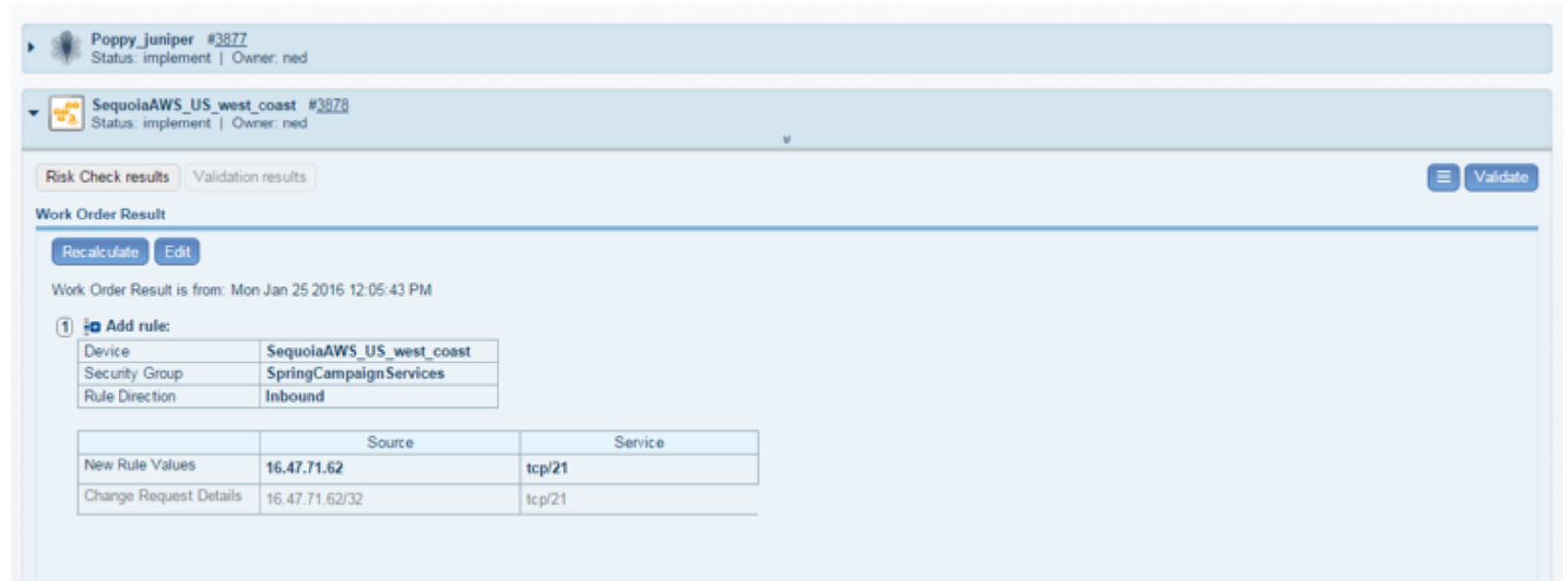
The screenshot displays the AlgoSec interface for migrating a Time Clock Server from LAX to AWS. The main window is titled "Moving Time Clock Server from LAX to AWS" and includes a "CANCEL" button and an "Update Applications" button. Below the title, there are sections for "Affected Applications", "Existing drafts to update", and "New drafts to create (1/1)". The "New drafts to create" section shows a draft for "Payroll" with a date of "09/11/2015", a status of "Production", and an "Active" flag. The draft details include a table with columns for "ID", "Source", "Destination", and "Action". The table shows a draft for "DC Time Clock Server" with a source of "LAX time clock server" and a destination of "Amazon cloud time clock server". The action is "Send time clock reports to the cloud time server (Planned to be migrated to AWS Data Center)".

| ID | Source               | Destination                    | Action   |
|----|----------------------|--------------------------------|--|
| 1  | DC Time Clock Server | Amazon cloud time clock server | Send time clock reports to the cloud time server (Planned to be migrated to AWS Data Center) |

The interface also shows a network diagram with a sidebar on the left listing "Devices in Path" under "BLOCKING (4)" and "ALLOWING (2)". The "BLOCKING" list includes "Rose\_checkpoint", "Rose\_DR", "Poppy\_juniper", and "SequoiaAWS\_US\_west\_coast". The "ALLOWING" list includes "DC\_42" and "DC\_82".

# APPLICATION MIGRATION

AlgoSec designs and provisions new cloud security controls, including risk assessment, validation and documentation



The screenshot displays the AlgoSec web interface. At the top, there are two navigation items: 'Poppy\_juniper #3877' with status 'implement' and owner 'ned', and 'SequoiaAWS\_US\_west\_coast #3878' with status 'implement' and owner 'ned'. Below these, there are tabs for 'Risk Check results' and 'Validation results', with a 'Validate' button on the right. The main section is titled 'Work Order Result' and contains 'Recalculate' and 'Edit' buttons. A message states 'Work Order Result is from: Mon Jan 25 2016 12:05:43 PM'. Underneath, there is an 'Add rule:' section with a table:

|                |                          |
|----------------|--------------------------|
| Device         | SequoiaAWS_US_west_coast |
| Security Group | SpringCampaignServices   |
| Rule Direction | Inbound                  |

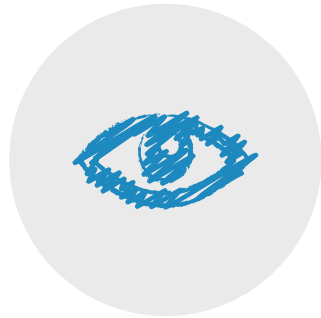
Below this is another table with columns for 'Source' and 'Service':

|                        | Source         | Service |
|------------------------|----------------|---------|
| New Rule Values        | 16.47.71.62    | tcp/21  |
| Change Request Details | 16.47.71.62/32 | tcp/21  |

Save months of manual labor!



# ALGOSEC'S HYBRID APPROACH



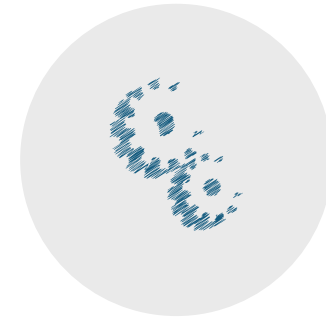
## Visibility

A single pain of glass across the organization's entire estate



## Compliance

Risk assessment and compliance reporting across the hybrid environment.



## Orchestration & automation

Automated & orchestrated across any heterogeneous environment

# 아마존 클라우드 보안관리

**MZ** Cloud Innovator  
**MEGAZONE**

aws partner network

algosec

**AWS ASIA NO.1 CONSULTING PARTNER**

**SECURITY MANAGEMENT PARTNER**

메가존, 보안 관리 솔루션 알고섹(AlgoSec)과 독점 파트너십 체결

# THANK YOU

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

