

MANAGE SECURITY
AT THE SPEED OF BUSINESS

보안정책 자동화와 워크플로우의 중요성

알고섹코리아 탁정수

 algosec



오늘날 보안 위협 통계

SECURITY



99%

Of firewall Breaches are the Result of Misconfiguration. Not firewall Flaws

AVAILABILITY



80%

8 out of 10 organizations Suffered an outage from a Misconfigure firewall rule In the last year

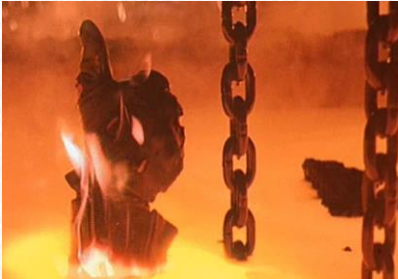
AGILITY



31%

Take an AVERAGE Of more than a day to perform a SINGLE connectivity change.

RISKS DO NOT JUST GO AWAY

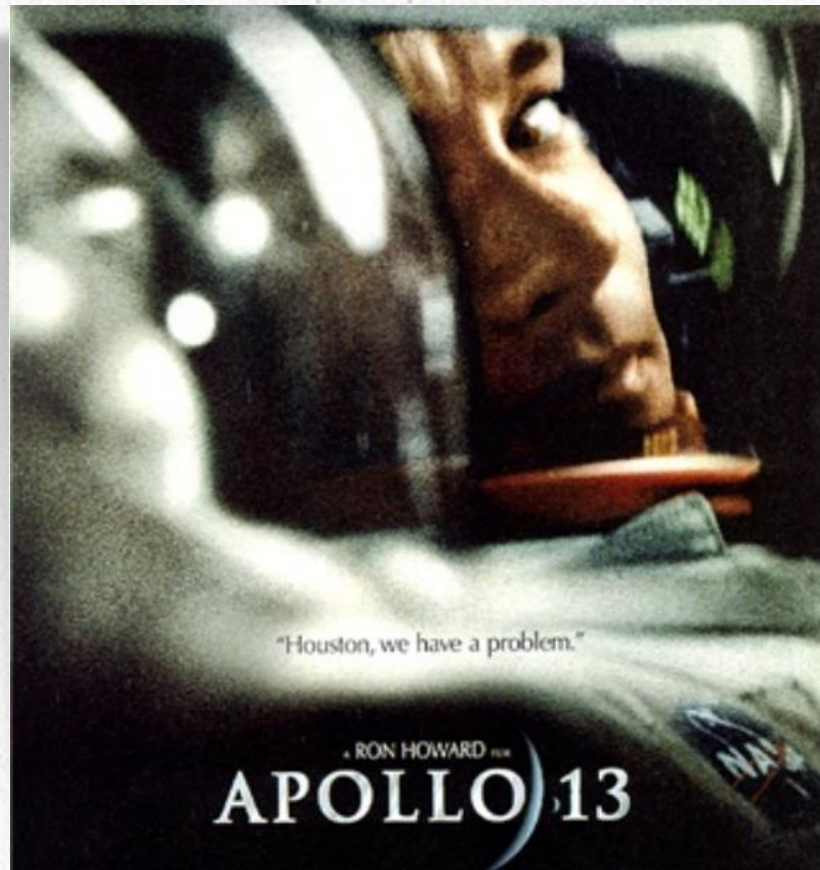


" I'll be Back "

- Understand Risk Level
- Risk Management Framework
- Relate Risk to Business Owner
- Mitigate
(Accepted risks stay in your network)
- Detect
- Understand Impact
- Respond Quickly
- Damage Control

FOCUS ON THE RIGHT PROBLEMS

"HOUSTON, WE HAVE A PROBLEM"



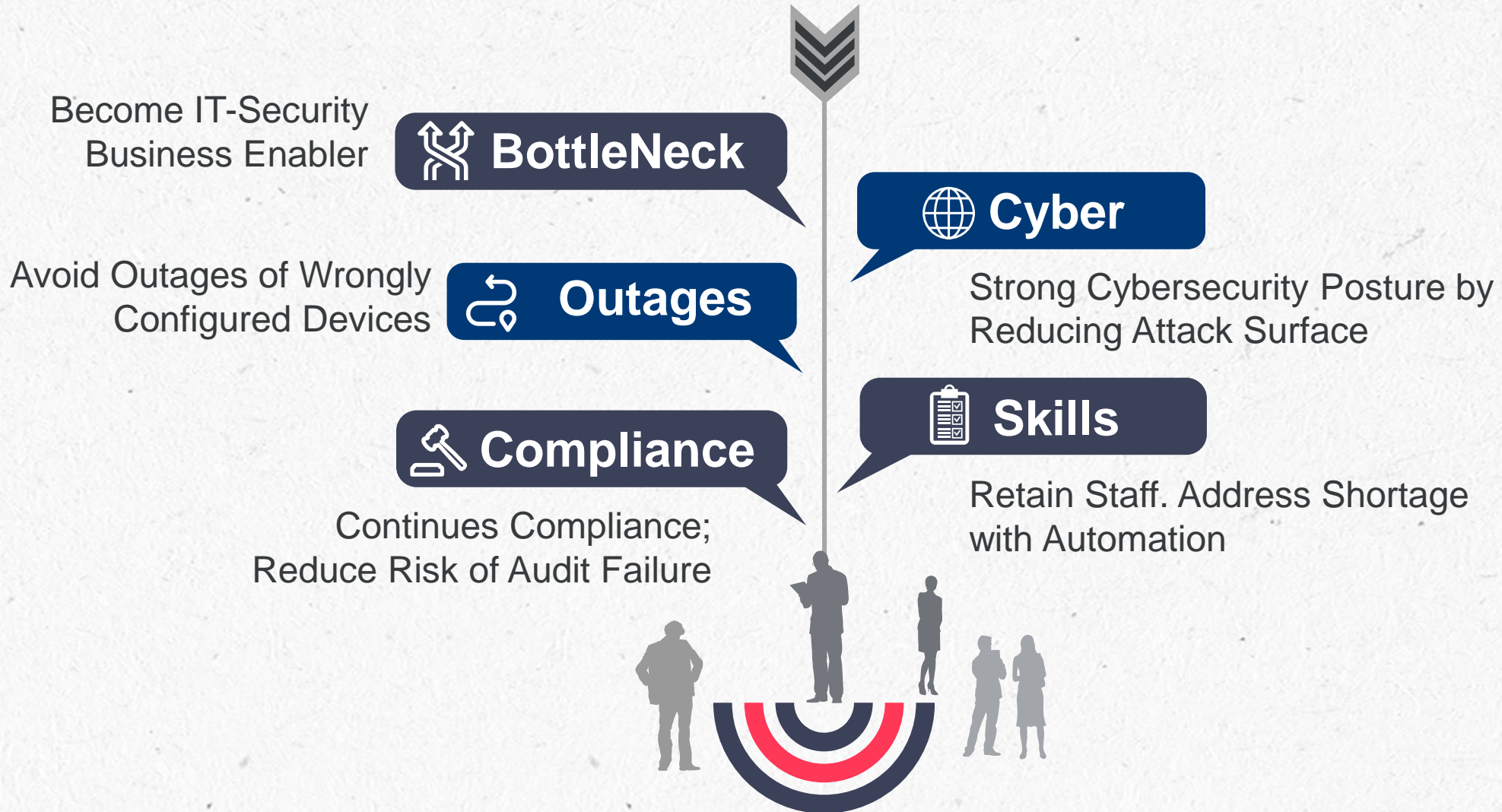
Speed of Business & Team Motivation

"I Feel the Need, Need for Speed"



- 비즈니스 변경속도를 따라잡기
- 새로운 어플리케이션 적용시간 : 수개월~수주
- 프로세스 변경에 대부분 시간 – 보안아키텍트
- 기술력 부족 – CIO 설문

5가지 위험 포인트와 방안



Cybersecurity Posture를 강화하라



“95% of Firewall Breaches from misconfiguration”



Ensure “basic” security hygiene. An optimized network security policy is critical to mitigating risk and cyberattacks



Automation & enforcing processes proved to be more effective than deploying incremental security technologies

Visibility and Automation



BottleNeck



Manual security processes have become a bottleneck to enabling business

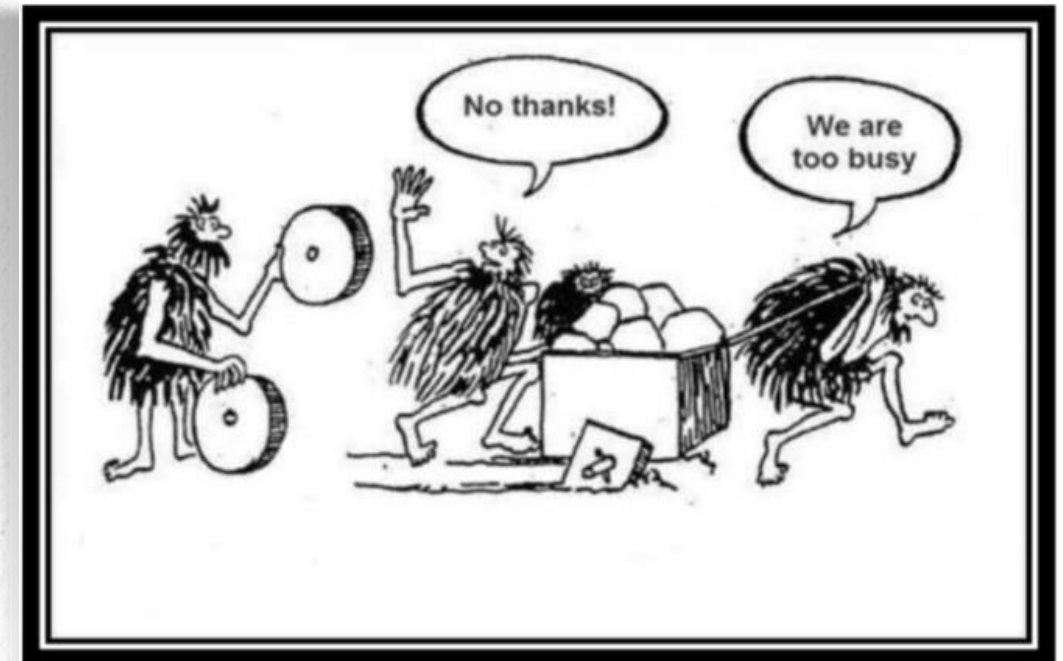


Firewall provisioning for a new application can take weeks



Cloud and SDN continue to add Pressure on security to be agile and operate at the “speed of business”

Business Focus



Skills



Security suffers from a serious talent shortage now and in the foreseeable future

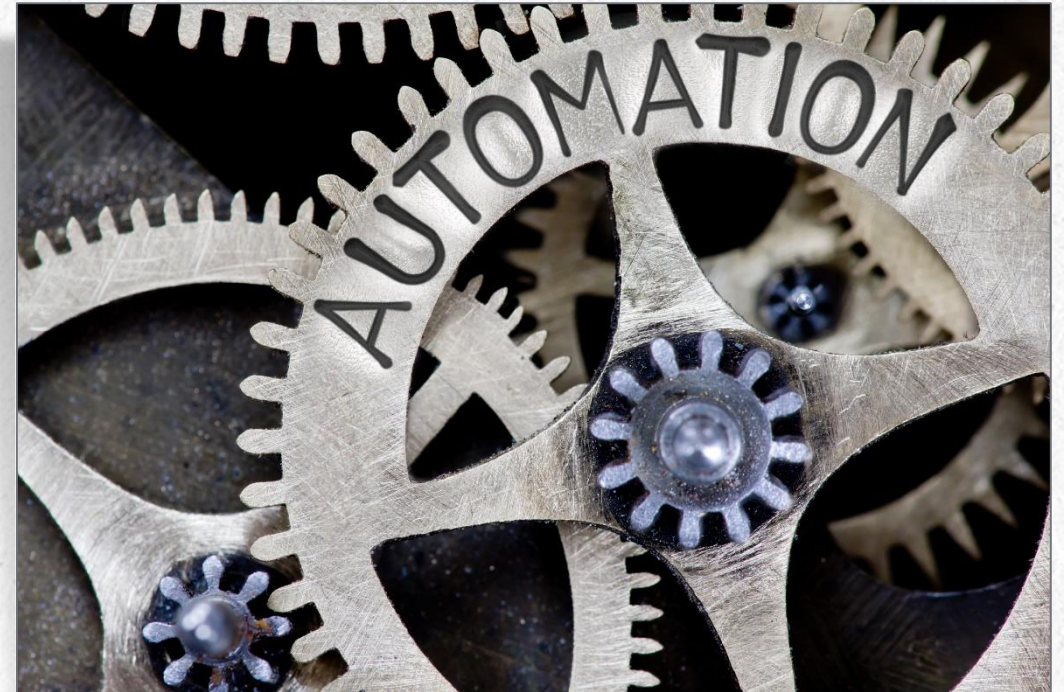


Difficult to ramp up new employees, as many senior engineers have all the “tribal knowledge”





Senior engineers pulled in too many directions

Automation



Outages



-  Security suffers from a serious talent shortage now and in the foreseeable future
-  Difficult to ramp up new employees, as many senior engineers have All the “tribal knowledge

*Source: “Digital Business Forever Changes How Risk and Security Deliver Value,” Gartner©

Compliance



Audit costs continue increasing together with network complexity



Greater challenges ensuring organizational policy across cloud platforms



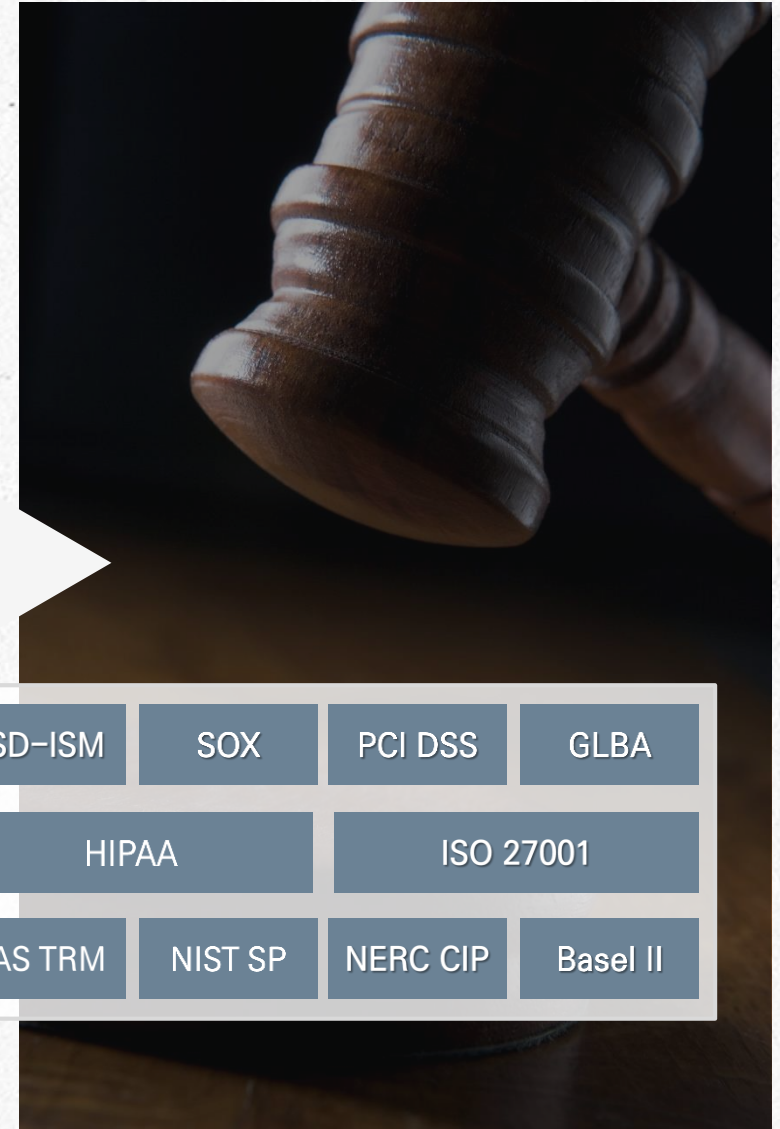
Audit failure cost is Huge – Automatic product will cost 10% or less



Avoid personal career implications...



Automation solution will many times make the Auditors 'go away' understanding you monitor compliance daily or weekly



ASD-ISM	SOX	PCI DSS	GLBA
HIPAA		ISO 27001	
NAS TRM	NIST SP	NERC CIP	Basel II

요약하면 3가지가 중요

1
See & Understand
what you are doing



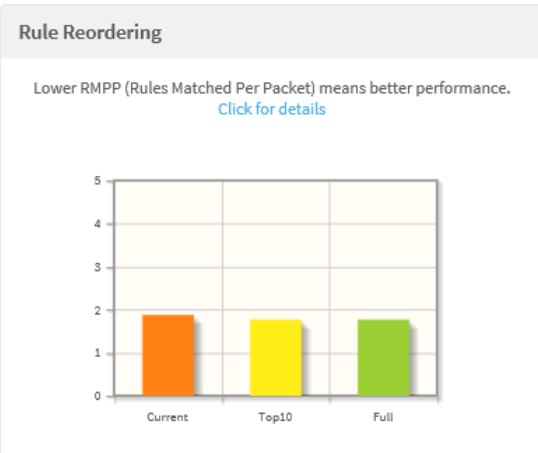
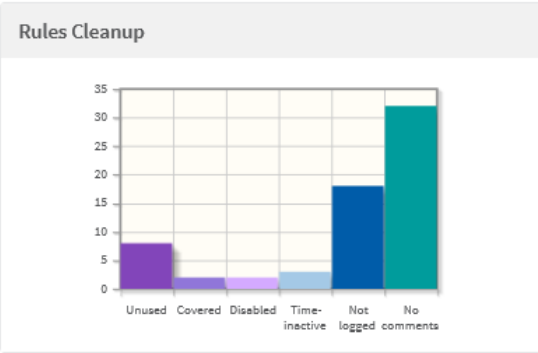
2
Prioritize well while keeping
“eyes on the ball”



3
Business Enablement,
Significant Costs Reduction,
Talent Retention, Increase
Accuracy & Efficiency



1. 정책 최적화, 변경 권고 기능 (Policy Optimization)



Rules Cleanup

Unused rules	8
Covered rules	2
Redundant special case rules	2
Consolidate rules	2
Unrouted rules	3
Unrouted objects within rules	1
Disabled rules	2
Time-inactive rules	3
Rules without logging	18
Rules with empty comments	32
Rules with non-compliant comments	0
Rules with a time clause	4
Rules about to expire	0
Rules	36

Objects Cleanup

Unattached objects	13
Empty objects	0
Duplicate objects	4
Unused objects within rules	3
Hostgroup definitions	104
Duplicate services	2

Intelligent Policy Tuner

Tighten Permissive Rules	5
Unused objects within rules	3
Policy tuner analysis for all rules	36

Rule Reordering

	RMPP	Improvement
Top 10 Optimizations	1.77	5%
Full Optimization	1.77	5%
Current Rule Order	1.88	

1. 정책 최적화, 변경 권고 기능 (Policy Optimization)

Intelligent Policy Tuner

The analysis is based on logs from 10-Nov-2016 to 12-Sep-2017. Log analysis is configured to include logs starting at midnight. To change this setting (unlimited): login as administrator and go to Administration > Options > Log Analysis

Policy: Pecan_after.paloalto

The table displays the density of the actually used IP addresses. No icons will be displayed in a rule that contains an IP address.

- Has no traffic log data associated with it.
- Is part of a rule that changed after the last traffic analysis.

If an object is sparsely used and includes many unused objects then it is a candidate for security tightening by refining the rule. The names of such sparse objects are highlighted. If an object is densely used then it is probably well defined. Press on any object's link for more details.

Legend: ■ - Unused ■ - Sparse ■ - Semi-Dense

NAME	FROM	SOURCE
http_based	demo_internal	Remote-30-internal_53
social_net	demo_internal	Inter_grp_30
yahoo	any	any
FTP_server	demo_internal	any
Cobra_app	any	any

Showing 1 to 5 of 5 entries

Intelligent Policy Tuner Recommendation

AlgoSec recommends to modify rule social_net to make it tighter and more secure. The suggested rule allows all the traffic that actually uses rule social_net according to the logs. AlgoSec attempts to re-use existing objects and services in its recommendation. If the firewall does not have suitable objects and services, then AlgoSec recommends their creation. Note that the suggested rule may possibly be tightened even further, using more complex definitions: detailed object and service usage information appears further down.

Please modify rule social_net, by removing unused objects, and replacing sparsely-used objects with tighter ones, so the rule looks as follows.

NAME	FROM	SOURCE	USER	TO	DESTINATION	APPLICATION	SERVICE	ACTION	COMMENT
social_net	demo_internal	Remote-30-internal_3	any	demo_dmz	DMZ_grp10.110	New_Application_1	New_Service_2	allow	

Highlighted objects and services indicate areas where you need to modify the rule. The definition details for any new objects and services you need to create appear below - please provide suitable names for them.

SERVICE NAME	SERVICE DEFINITION
New_Service_2	tcp/787 udp/907 udp/65 tcp/1008 udp/124 udp/673 tcp/179

APPLICATION NAME	APPLICATION DEFINITION
New_Application_1	facebook-posting facebook-base facebook-chat facebook-mail facebook-social-plugin

Intelligent Policy Tuner traffic breakdown

Rule Source

NAME	IP SUBNET / ADDRESS	COUNT	LAST USE	PERCENTAGE	OBJECT
Inter_grp_30	10.30.73.9	274,662,640	11Jan2017	100%	Remote-30-internal_3
	10.30.73.5				
	10.30.73.15				
	10.30.73.53				

An existing object that includes all the used IP addresses: Remote-30-internal_3 (may also include some unused addresses)

Rule Destination

NAME	IP SUBNET / ADDRESS	COUNT	LAST USE	PERCENTAGE	OBJECT
DMZ_grp10.110	10.110.73.11-10.110.73.11	234,419,200	11Jan2017	100%	

Rule Service

NAME	SERVICES	COUNT	LAST USE	PERCENTAGE	OBJECT
any	tcp/179	131,814,124	11Jan2017	47.95%	
	tcp/787	271,164	11Jan2017	0.1%	
	tcp/1008	2,303,278	11Jan2017	0.84%	
	udp/65	4,163,200	11Jan2017	1.51%	
	udp/124	81,816,184	11Jan2017	29.83%	
	udp/673	54,800,996	11Jan2017	19.93%	
	udp/907	905,104	11Jan2017	0.33%	
	icmp/0-255				
	tcp/0-178				
	tcp/1009-8555				
tcp/180-798					
tcp/788-1007					
udp/0-64					
udp/125-672					
udp/65-123					
udp/674-906					
udp/900-8553					
Other Services					

Rule Application

NAME	APPLICATIONS	COUNT	LAST USE	PERCENTAGE	OBJECT

2. 네트워크 토폴로지 맵의 정확성 및 트래픽 시뮬레이션 쿼리

The screenshot displays the Firewall Analyzer interface. On the left, a sidebar lists various devices under the 'ALL_FIREWALLS' group, including Data_Center_42, Data_Center_82, Acorn_ASA, and others. The main area shows the configuration for a 'Traffic Simulation Query' for the 'ALL_FIREWALLS' group. The configuration includes fields for Source, User, Destination, Application, and Service, each with an 'Add...' button. A 'NAT Discovery' button is also present. A 'Discover NAT Assistant' dialog box is overlaid on the right, prompting the user to 'Type a single IP' (with an example '192.168.2.3') and to check options for 'Pre-NAT', 'Post-NAT', 'Source', and 'Destination'. Below the dialog, a network topology map is visible, showing devices like '10.42.18.80/30', '10.42.65.96/28', and 'teak_fs' connected to a central 'Violet_Fortinet' device. The interface also shows a 'Latest Report' for Sep 12, 2017, and a 'Number of devices: 2' indicator.

3. 보안 정책 적용 자동화

ActiveChange 기능

#2182 access to Coyote system

Plan Approve Implement Validate Match

Messages

- To implement the change, please update Rose_checkpoint configuration as planned, then proceed to the next workflow step.

Rose_checkpoint
Status: Implement, Owner: ned, ID: #2182

Validation results

Work Order Result

Recalculate Edit

The device's policy has been updated after the below Work Order was created. It is policy.

Work Order Result is from: Thu Aug 22 2013 2:45:43 PM

1. Add rule:

Device	Rose_checkpoint
Refer to Rule Number	32 View Policy

	Source	Destination	Service	Action	Rule Name
New Rule Values	RachelPC	COYOTE3	RPC-Mapper	accept	FireFlow #2182
Change Request Details	16.47.71.62	10.176.67.101	tcp/136	accept	

Implement On Device

Work Order Result

Work Order Result is from: Tue Jul 14 2015 7:19:34 am

1. Add rule:

Device	10.128.1.36
ACL	acl_out

	Source	Destination	Service	Action	Description
New Rule Values	4.2.2.2	10.128.78.100	any	permit	FireFlow #10
Change Request Details	4.2.2.2	10.128.78.100	*	permit	

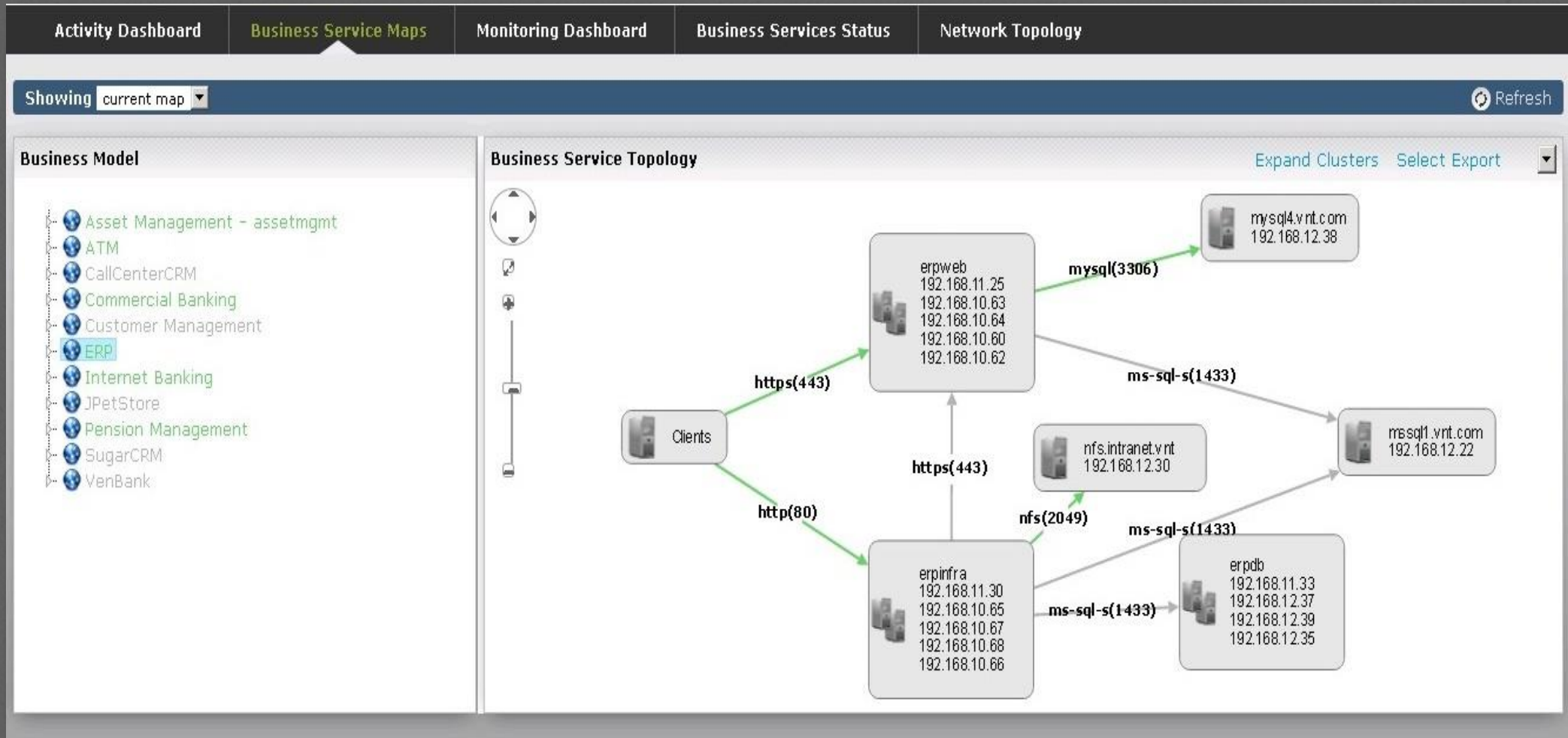
Details

CLI Recommendation

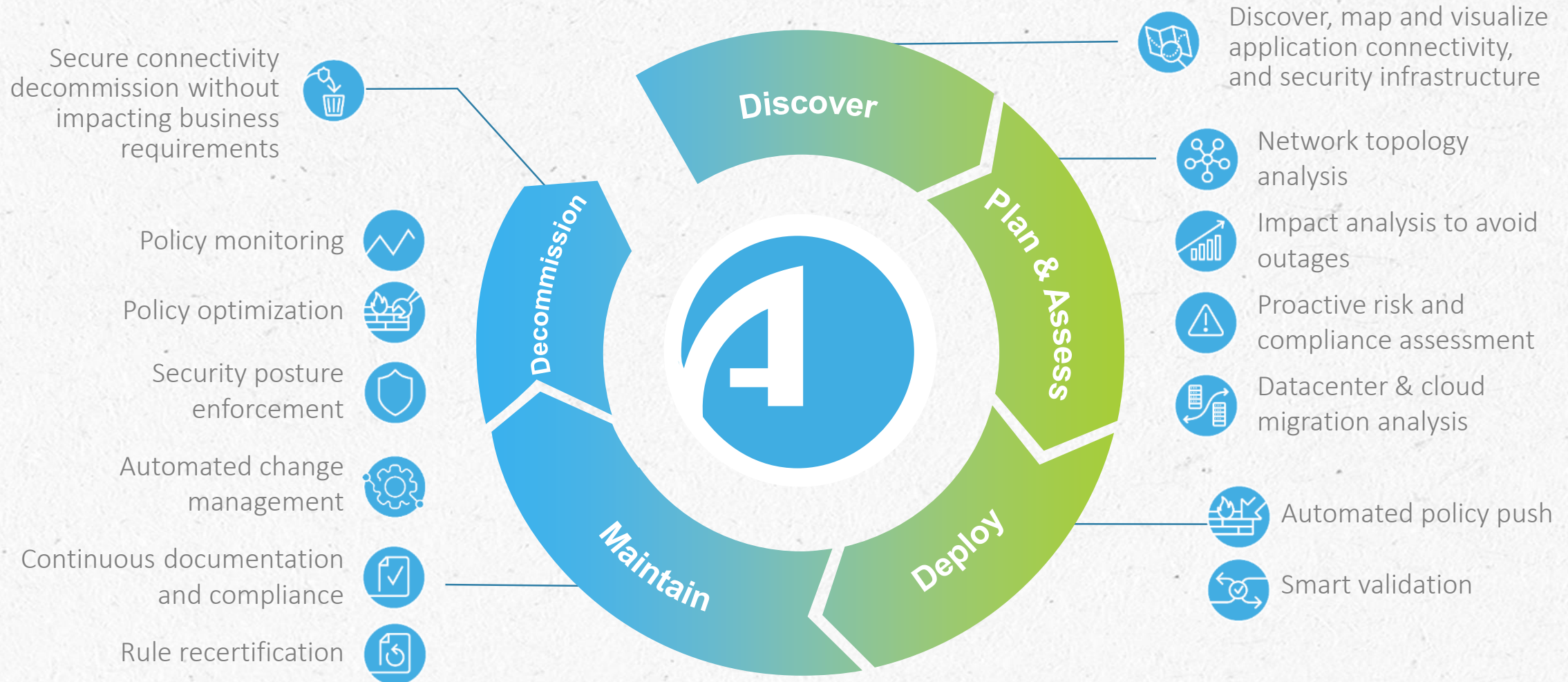
```
access-list acl_out remark FireFlow #10
access-list acl_out extended permit ip host 4.2.2.2 host 10.128.78.100 log
```

변경을 위한 최적 규칙 제시

4. 어플리케이션의 연결성 및 가시성 정보



THE SECURITY POLICY MANAGEMENT LIFECYCLE



About AlgoSec...



2004 설립



전 세계 1,700여 고객



Fortune 50대 기업 중 30개 고객



3개의 글로벌 센터를 통한 24/7 지원



Global No.1 Market Share



MANAGE SECURITY
AT THE SPEED OF BUSINESS

THANK YOU

www.algosec.com

