ALGOSEC CLOUD SECURITY MANAGEMENT

Presenter name

Date

BUSINESS-DRIVEN
SECURITY MANAGEMENT

algosec CLOUD

CORPORATE OVERVIEW

Founded in 2004

1800+ Enterprise Customers

Serving 20 of the Fortune 50

24/7 Support via 3 Global Centers

Passionate about Customer Satisfaction

NASDAQ ORACLE GM Chevron at&t intel BT VW bp STATE STREET ERICSSON

skype RBC hp SONY Unilever orange usbank Microsoft ESTĒE LAUDER ENBRIDGE

TIME WARNER CABLE Office DEPOT BED BATH & BEYOND HALLIBURTON BANK OF ENGLAND Dominion 招商银行 ING

algosec CLOUD

BUSINESS-DRIVEN SECURITY MANAGEMENT

Business-Driven Network Security Policy Management

Business-Driven Security

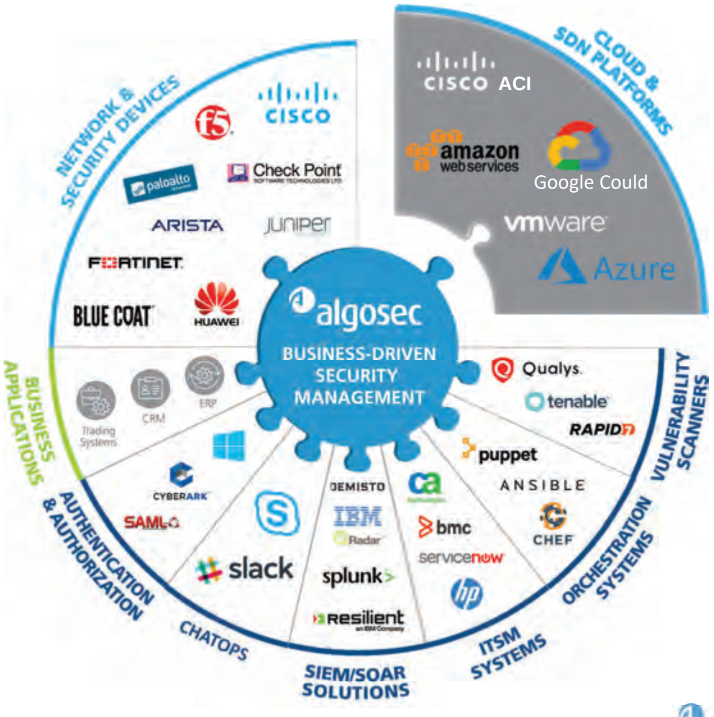
Business-Driven Agility

Unified Visibility Across Cloud, SDN & On-Premise Enterprise Networks

USE CASES

- Change Management
- Risk Management
- Auditing & Compliance
- Incident Response
- Micro-Segmentation
- DevOps
- Business Continuity
- Cloud Migration
- Digital Transformation

THE ALGOSEC ECOSYSTEM

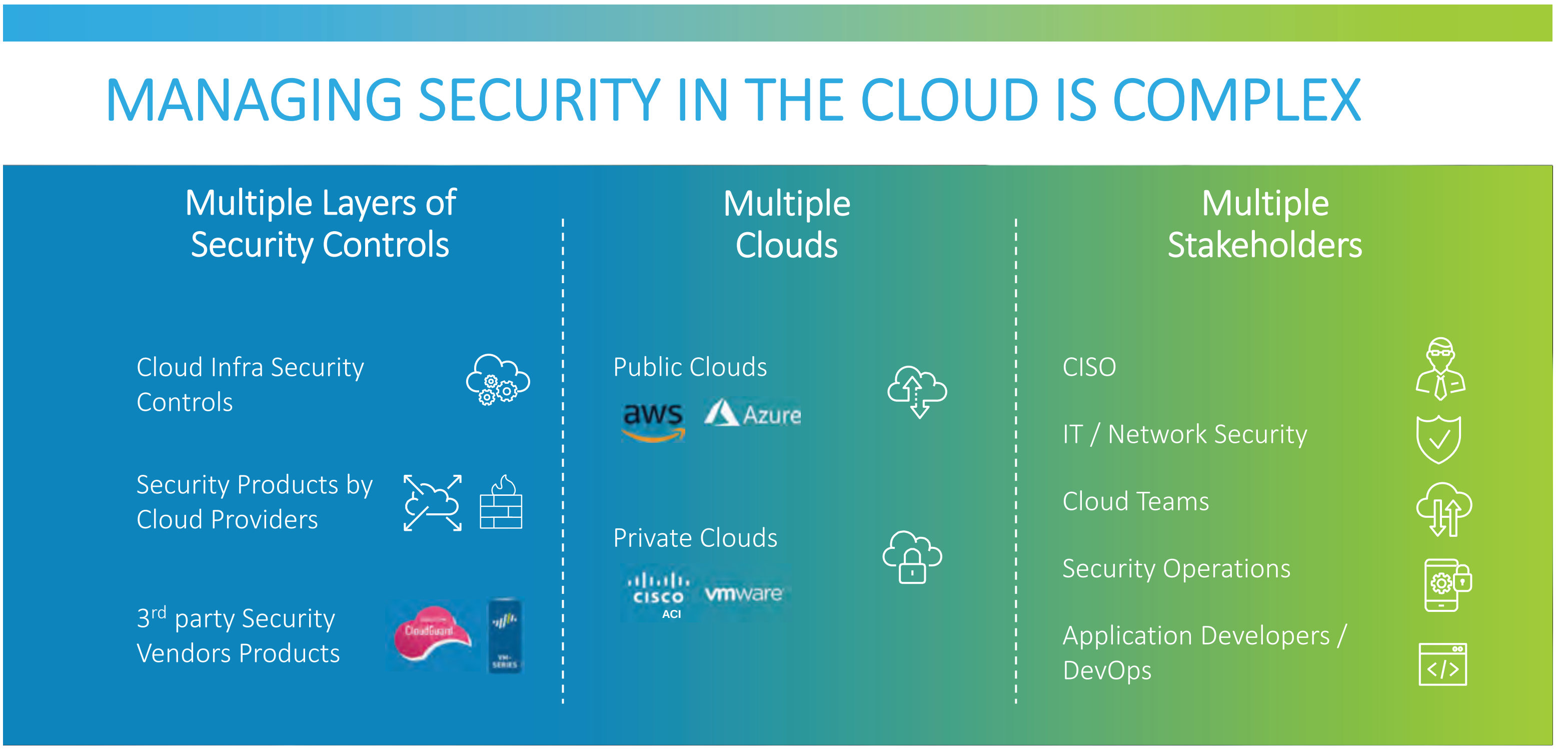


Manage

Business Process

Integrate

For a complete list of supported devices visit www.algosec.com



MANAGING SECURITY IN THE CLOUD IS COMPLEX

Multiple Layers of Security Controls

Cloud Infra Security Controls

Security Products by Cloud Providers

3rd party Security Vendors Products

Multiple Clouds

Public Clouds

aws Azure

Private Clouds

cisco ACI vmware

Multiple Stakeholders

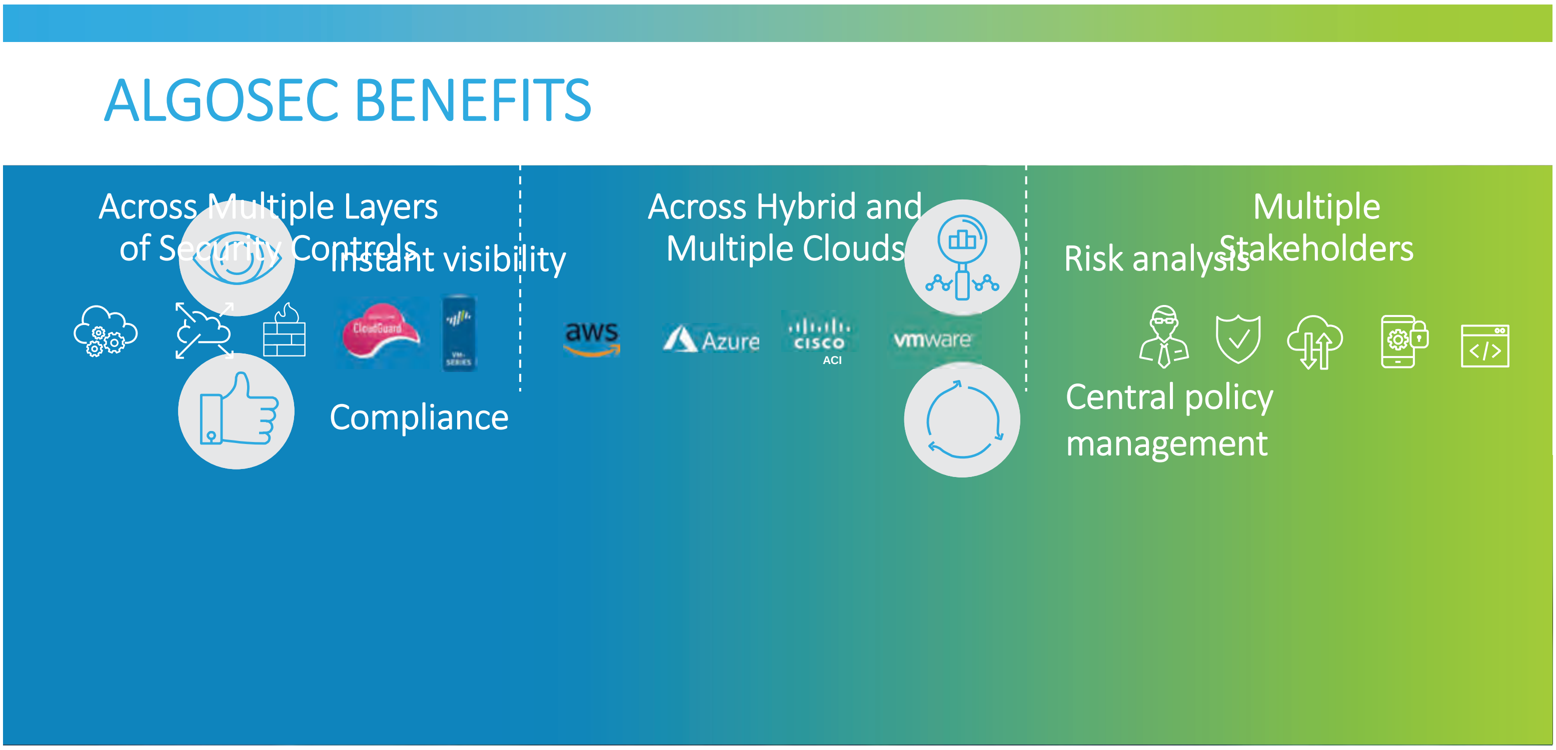
CISO

IT / Network Security

Cloud Teams

Security Operations

Application Developers / DevOps



ALGOSEC BENEFITS

Across Multiple Layers of Security Controls

Instant visibility

Compliance

Across Hybrid and Multiple Clouds

aws Azure cisco ACI vmware

Multiple Stakeholders

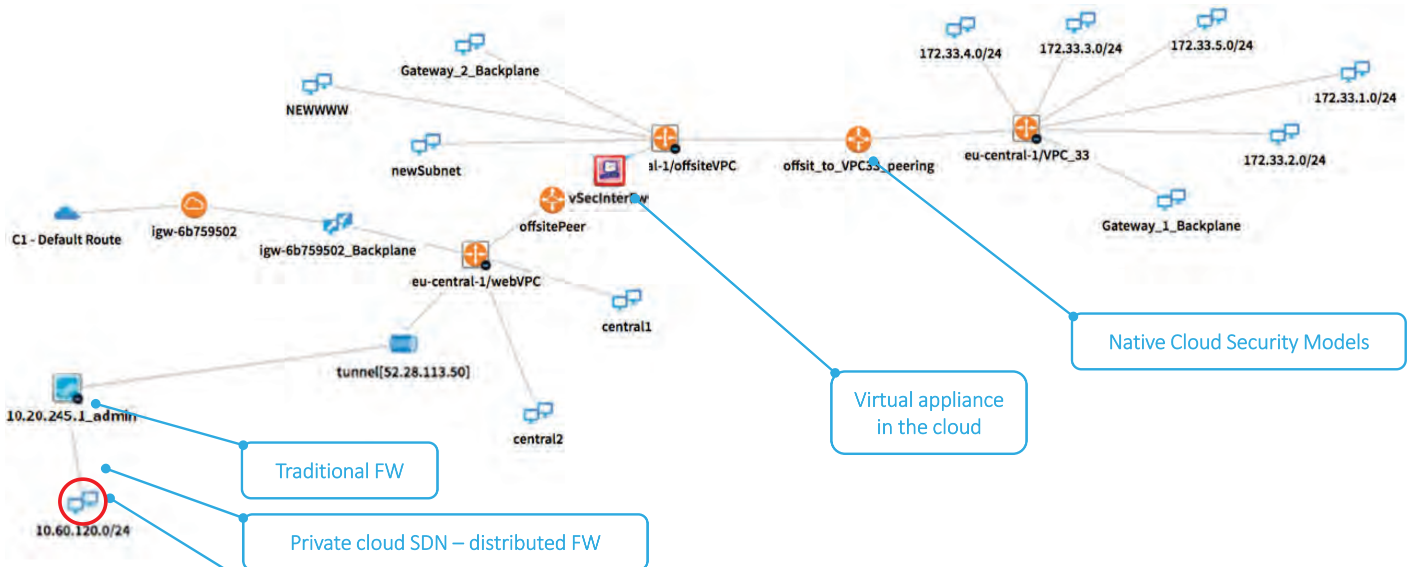
Risk analysis

Central policy management

SECURE CONNECTIVITY PROVISIONING FOR YOUR CLOUD MIGRATIONS

- Automatically discover and map application
- What-if risk assessment and compliance reporting
- Assess the changes in application connectivity requirements
- Automatically migrate the connectivity flows to the new AWS environment
- Securely decommission old connectivity
- Ongoing monitoring and visibility of the hybrid cloud

MANAGE HYBRID CLOUD WITH E2E VISIBILITY



Native Cloud Security Models

Virtual appliance in the cloud

Traditional FW

Private cloud SDN – distributed FW

Virtual appliance in the SDN arena

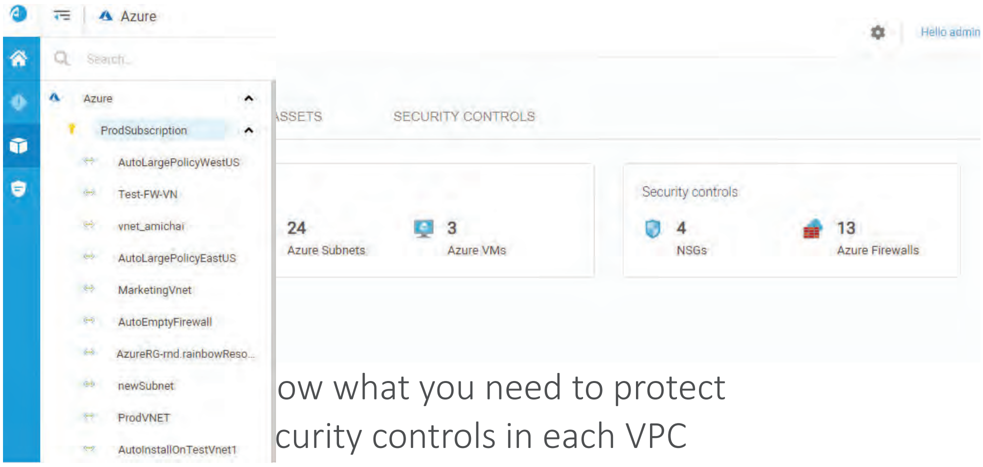
VISIBILITY INTO YOUR CLOUD ESTATE

01 Know what you need to protect

02 Security controls in each VPC

03 Change monitoring

04 Easy navigation



ow what you need to protect

curity controls in each VPC

- Change monitoring
- Easy navigation

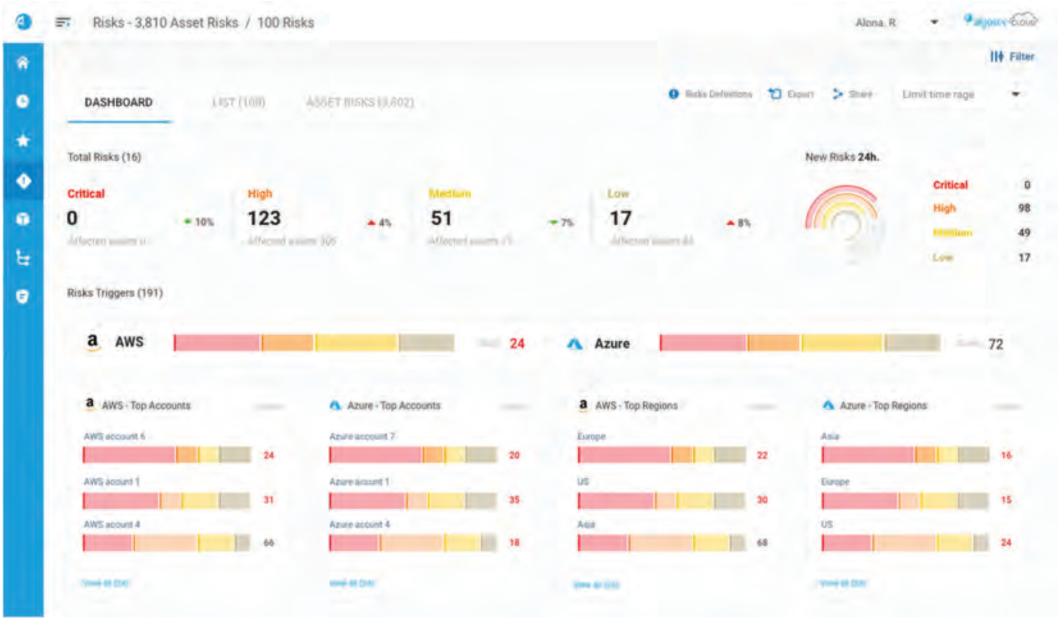
algosec CLOUD

MANAGE SECURITY RISKS OF CLOUD ASSETS

01 Risk notifications

02 At-a-glance security posture view

03 Actionable risk management



algosec CLOUD

MANAGE SECURITY RISKS OF CLOUD ASSETS

01

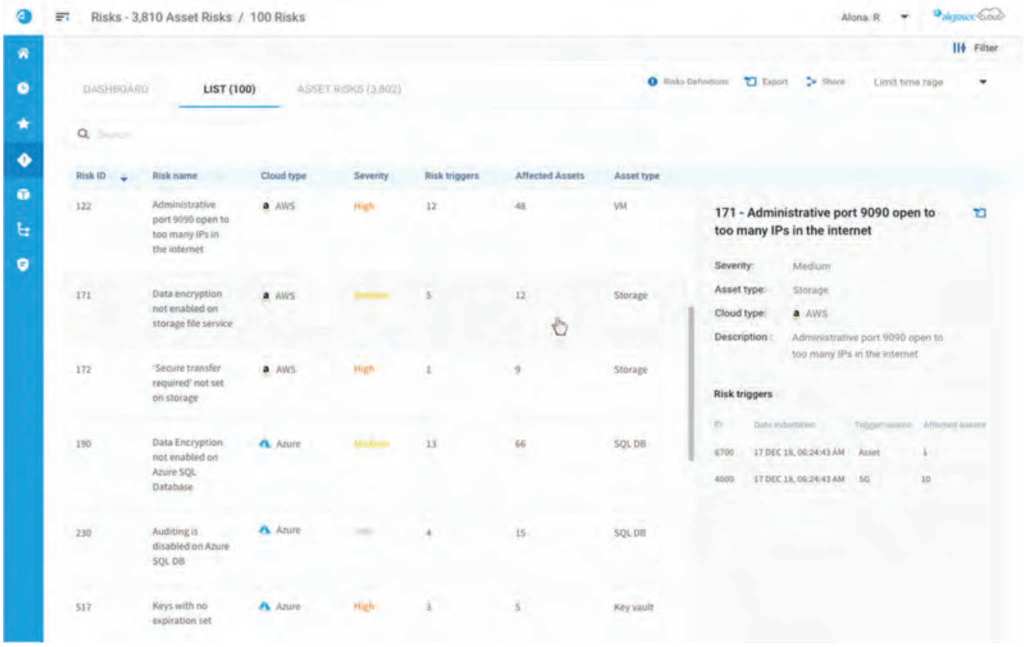
Risk notifications

02

At-a-glance security posture view

03

Actionable risk management



Risks - 3,810 Asset Risks / 100 Risks

Alona. R

Filter

DASHBOARD | LIST (100) | ASSET RISKS (3,802)

Risks Definitions | Export | Share | Limit time rage

Search

Risk ID	Risk name	Cloud type	Severity	Risk triggers	Affected Assets	Asset type
122	Administrative port 9090 open to too many IPs in the internet	AWS	High	12	48	VM
171	Data encryption not enabled on storage file service	AWS	Medium	5	12	Storage
172	'Secure transfer required' not set on storage	AWS	High	1	9	Storage
190	Data Encryption not enabled on Azure SQL Database	Azure	Medium	13	66	SQL DB
230	Auditing is disabled on Azure SQL DB	Azure	[illegible]	4	15	SQL DB
517	Keys with no expiration set	Azure	High	3	5	Key vault

171 - Administrative port 9090 open to too many IPs in the internet

Severity: Medium

Asset type: Storage

Cloud type: AWS

Description: Administrative port 9090 open to too many IPs in the internet

Risk triggers

ID	Date indentified	Trigger reason	Affected assets
6700	17 DEC 18, 06:24:43 AM	Asset	1
4000	17 DEC 18, 06:24:43 AM	SG	10

CENTRAL MANAGEMENT OF NETWORK POLICIES

01

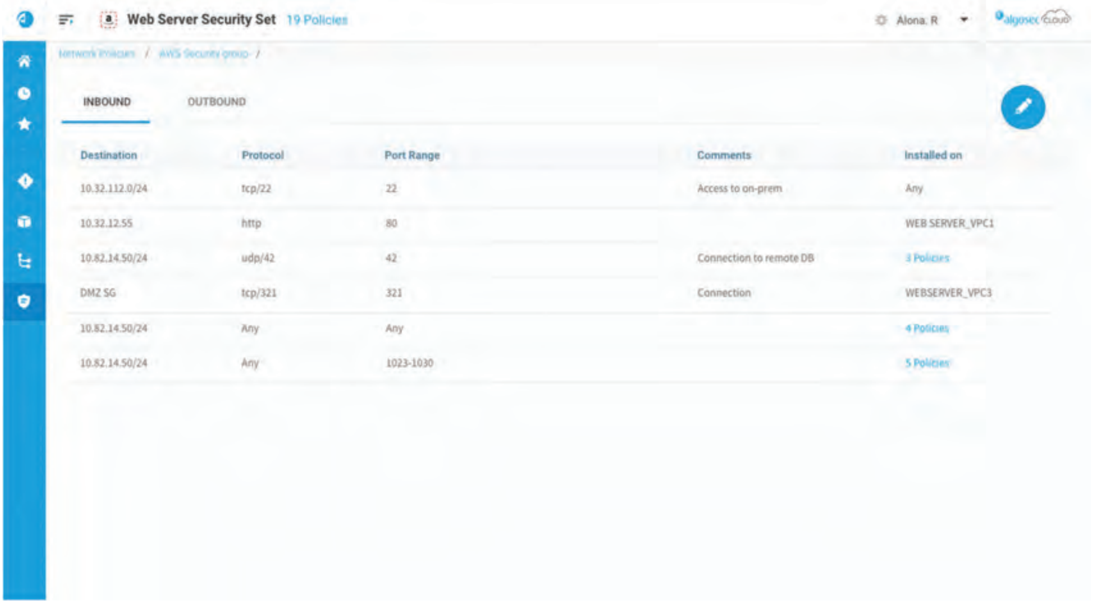
Across accounts, regions, VPCs, VNETS

02

Easy management of rules in similar SGs

03

Easy provisioning of on-prem network rules and virtual firewalls



Web Server Security Set 19 Policies

Alona. R

Network Policies / AWS Security group /

INBOUND | OUTBOUND

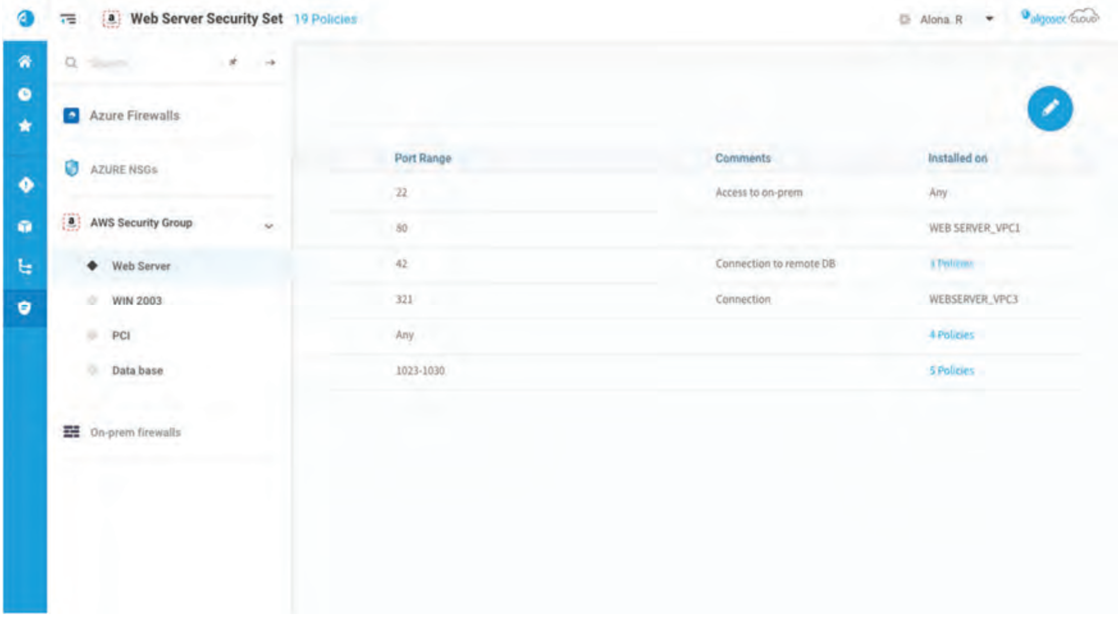
Destination	Protocol	Port Range	Comments	Installed on
10.32.112.0/24	tcp/22	22	Access to on-prem	Any
10.32.12.55	http	80		WEB SERVER_VPC1
10.82.14.50/24	udp/42	42	Connection to remote DB	3 Policies
DMZ SG	tcp/321	321	Connection	WEBSERVER_VPC3
10.82.14.50/24	Any	Any		4 Policies
10.82.14.50/24	Any	1023-1030		5 Policies

CENTRAL MANAGEMENT OF NETWORK POLICIES

01 Across accounts, regions, VPCs, VNETS

02 Easy management of rules in similar SGs

03 Easy provisioning of on-prem network rules and virtual firewalls



Web Server Security Set 19 Policies

Alona. R

Azure Firewalls

AZURE NSGs

AWS Security Group

- Web Server
- WIN 2003
- PCI
- Data base

On-prem firewalls

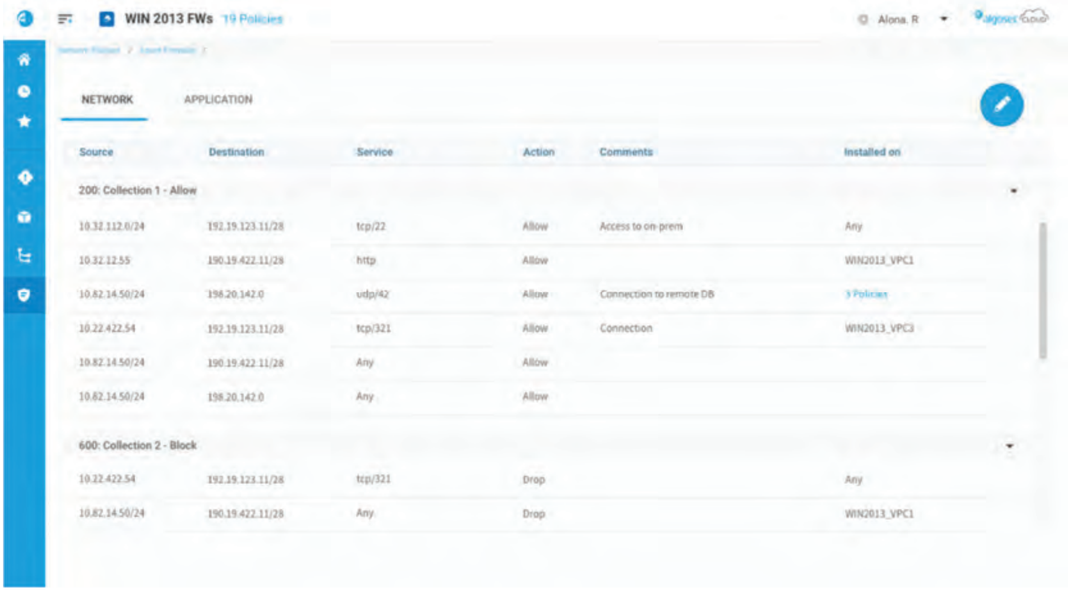
Port Range	Comments	Installed on
22	Access to on-prem	Any
80		WEB SERVER_VPC1
42	Connection to remote DB	3 Policies
321	Connection	WEBSERVER_VPC3
Any		4 Policies
1023-1030		5 Policies

CENTRAL MANAGEMENT OF NETWORK POLICIES

01 Across accounts, regions, VPCs, VNETS

02 Easy management of rules in similar SGs

03 Easy provisioning of on-prem network rules and virtual firewalls



WIN 2013 FWs 19 Policies

Alona. R

NETWORK APPLICATION

Source	Destination	Service	Action	Comments	Installed on
200: Collection 1 - Allow					
10.32.112.0/24	192.19.123.11/28	tcp/22	Allow	Access to on-prem	Any
10.32.12.55	190.19.422.11/28	http	Allow		WIN2013_VPC1
10.82.14.50/24	198.20.142.0	udp/42	Allow	Connection to remote DB	3 Policies
10.22.422.54	192.19.123.11/28	tcp/321	Allow	Connection	WIN2013_VPC3
10.82.14.50/24	190.19.422.11/28	Any	Allow		
10.82.14.50/24	198.20.142.0	Any	Allow		
600: Collection 2 - Block					
10.22.422.54	192.19.123.11/28	tcp/321	Drop		Any
10.82.14.50/24	190.19.422.11/28	Any	Drop		WIN2013_VPC1

SUMMARY: ALGOSEC CLOUD OFFERING

ASMS

Network security across the hybrid cloud

Cloud native network security and ISV firewalls in the cloud

- Visibility
- Change management automation

Cloud migration – networking provisioning

- Application flows discovery
- Project based network policy risk analysis and provisioning

CloudFlow

Protect cloud assets (not just networking)

- Risk analysis including beyond network rules

Central, cloud-oriented network policy management

- One view Across accounts, regions, VPCs (vnets)
- Azure FW

Full visibility into cloud estate

- Easily navigate your multi-cloud estate; Monitor changes

SUMMARY

- Cloud security is complex:
  - Multi-security controls
  - Problematic visibility
  - Multiple stake-holders
- Easy to achieve agility, harder to keep it secure
- AlgoSec is your partner for:
  - Connectivity provisioning for application migration
  - Risk and compliance
  - Central Security Policy Management
  - Support for hybrid cloud and multi-clouds

THANK YOU

algosec CLOUD