

**tufin**



**Henry Pea**

# Enterprise Network Security Challenges



## Complexity

Limited visibility and control for Next Gen networks spanning across physical and cloud platforms



## Change

Ever-changing policies introduce new attack vectors



## Cybersecurity

Cyber attacks must be contained



## Connectivity

Application connectivity is critical for the business



## Compliance

Regulators demand continuous compliance with security standards

# Tufin At-a-Glance



**Market Leader  
Security Policy  
Orchestration**



**> 1,900  
Customers  
Worldwide**



**Award-Winning  
Tufin Orchestration  
Suite™**



# Tufin Benefits

## Maximize Agility & Security with network security policy orchestration



Implement security changes in minutes instead of days



Ensure continuous compliance with security standards



Reduce complexity of managing hybrid networks

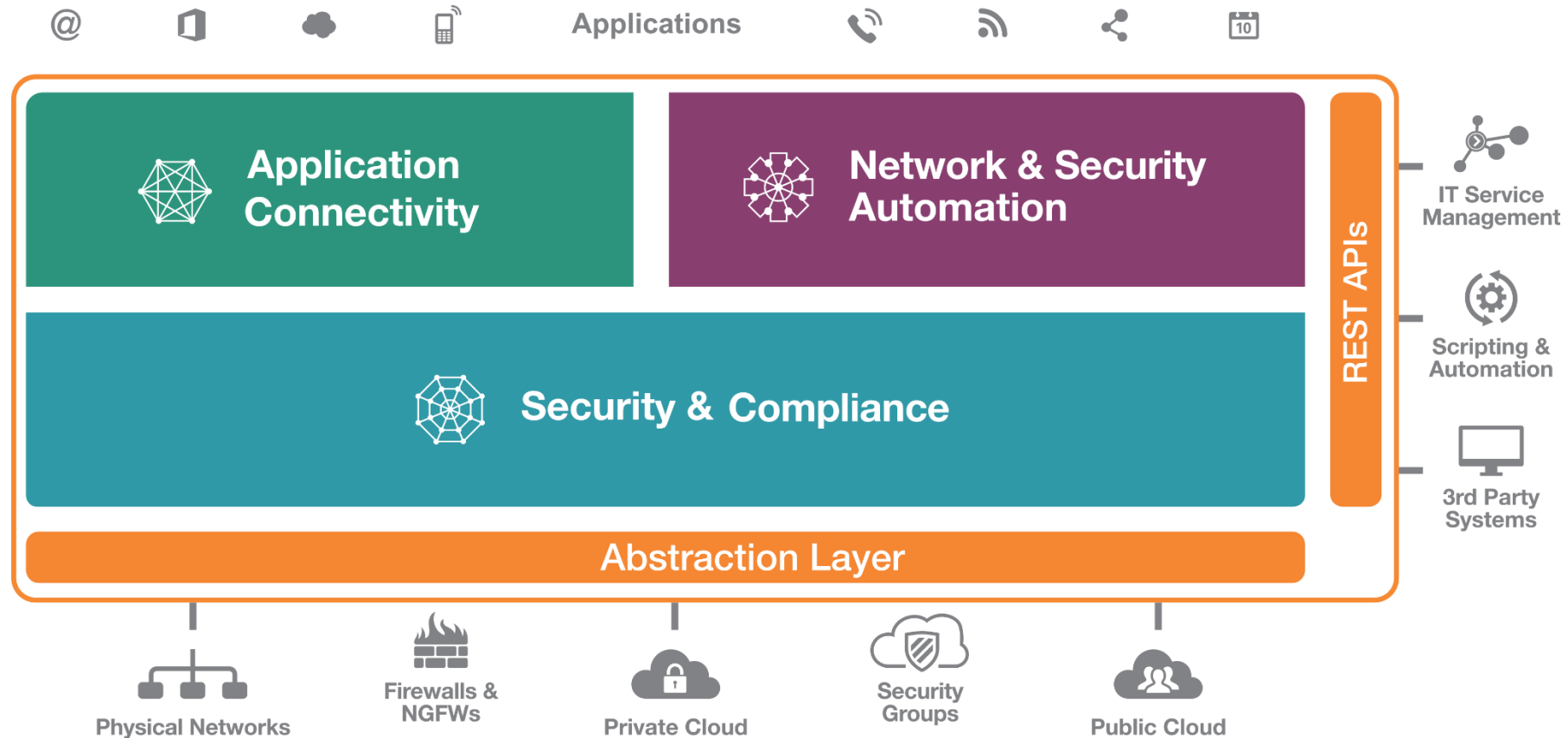
# The Tufin Vision

## The enterprise network-of-the-future



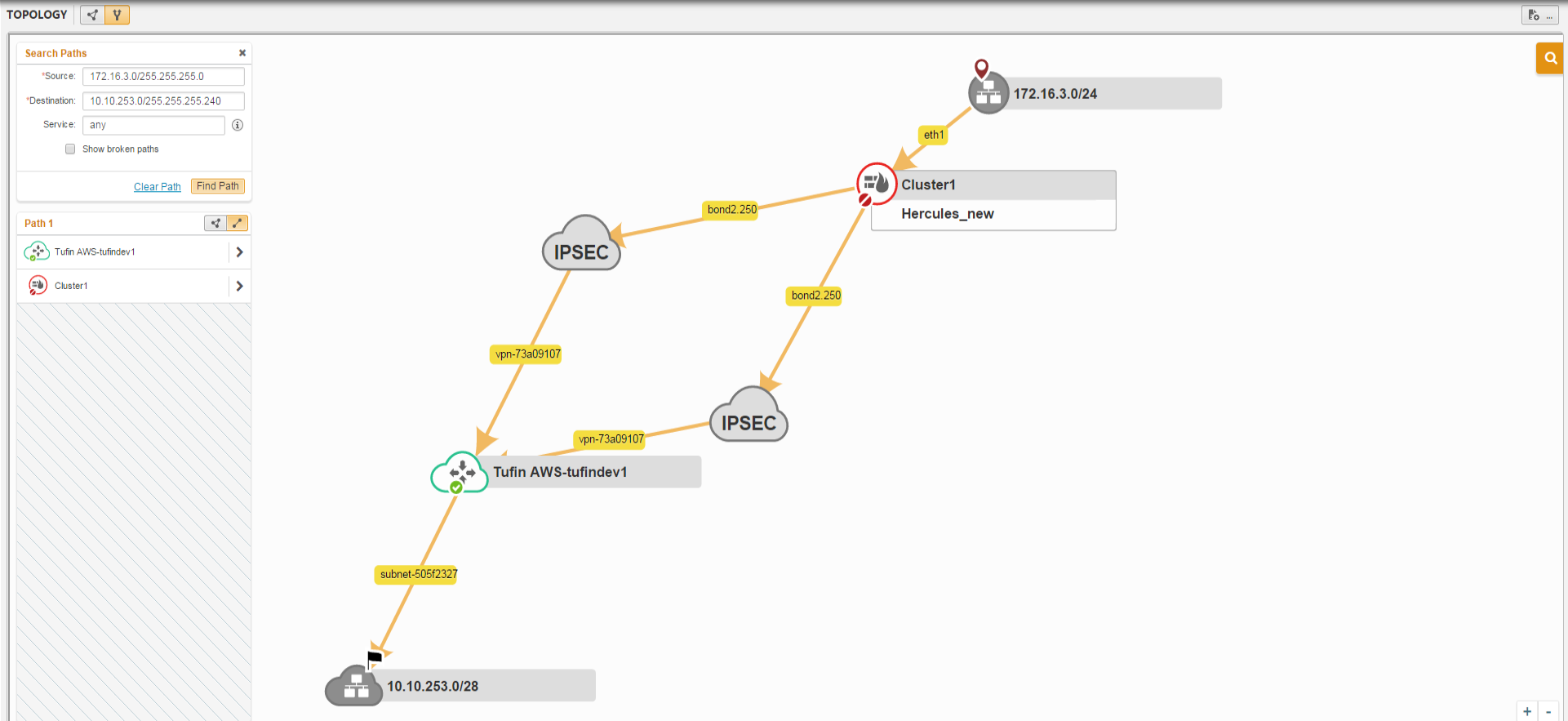
- **Network security changes will be predominantly automated** except for security exceptions review
- **A single, comprehensive enterprise network security policy**
- **Most data centers will move to public & private cloud** with a virtual network platform layer

# Tufin Orchestration Suite™



# Single Pane of Glass for Network Security

Visibility & control for analyzing security & connectivity  
across physical networks & hybrid cloud platforms



# Network Security Policy Baseline

Strengthen network security posture by defining & enforcing a corporate-wide zone-based policy across heterogeneous environments

UNIFIED SECURITY POLICY → Corporate Matrix (North - South Traffic)

From	To	Amsterdam_Ext	Amsterdam_SiteA	Amsterdam_SiteB	Cali_bckp-site	London	TexasVPN users	Toronto
Amsterdam_Ext								
Amsterdam_SiteA								
Amsterdam_SiteB								
Cali_bckp-site								
London								
p_DataCenter								
p_PM								
p_RnD								
p_Sales								
TexasVPN users								
Toronto								

**p\_PM to Cali\_bckp-site**

✓ **The following services are allowed:**  
https (tcp), ssh (tcp), tcp 3306, udp 53,  
tcp 67-68, tcp 389, tcp 445, SMTPS (tcp)

**Rule properties:**

- Rules must have explicit source (not ANY)
- Rules must have explicit destination (not ANY)
- Rules must have explicit service (not ANY)
- Rules must have comment
- Rules must be logged
- Rules must have hit within last 30 days
- Source must contain no more than 1 IP addresses
- Destination must contain no more than 1 IP addresses
- Service must contain no more than 1 services

**Flows:**  
Host → Host



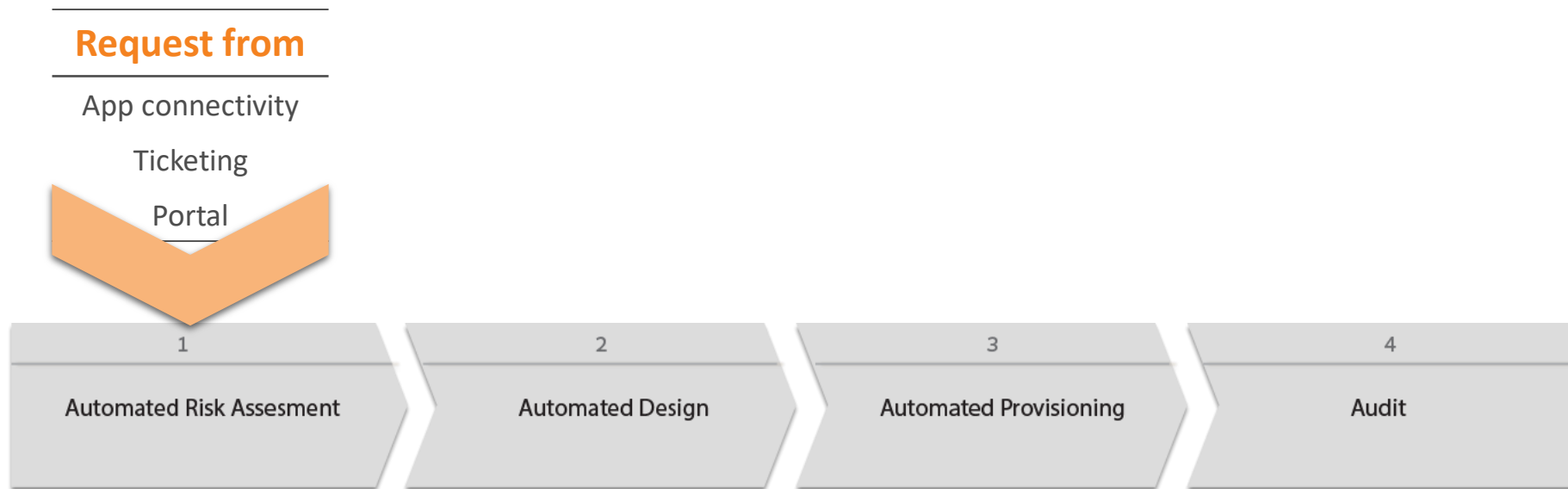
# Application Connectivity Model

Discover & manage connectivity needs of every application to increase agility, ensure business continuity & improve communication between App & Network Security teams



# Automated Network Security Change Process

Maximize agility with end-to-end automation of network security changes  
with baked-in security & compliance



# Automated Risk Analysis



Automated risk analysis for baked-in security & compliance

UNIFIED SECURITY POLICY → Corporate Matrix (North - South Traffic)

[Export...](#) [Import...](#)

From \ To	Amsterdam_Ext	Amsterdam_SiteA	Amsterdam_SiteB	Cali_bckp-site	London	p_DataCenter	p_PM	p_RnD	p_Sales	TexasVPN users	Toronto
Amsterdam_Ext		H	H	H	L	H	H	L	H	M	H
Amsterdam_SiteA	H		H	H	H	H	H	L	M	M	H
Amsterdam_SiteB	H	H		H	H	H	H	M	H	H	H
Cali_bckp-site	H	H	H		H	H	H	H	H	H	H
London	H	H	H	H		H	H	H	H	M	H
p_DataCenter	H	H	L	H	H		L	L	L	M	M
p_PM	H	H	H	H	H	H		L	L	H	H
p_RnD	H	H	H	H	M	H	L		L	H	H
p_Sales	H	C	M	H	M	H	L	L		H	H
TexasVPN users	H	H	C	H	H	C	H	H	H		H
Toronto	H	H	H	H	H	M	H	M	L	H	

# Automated Network Security Change Design



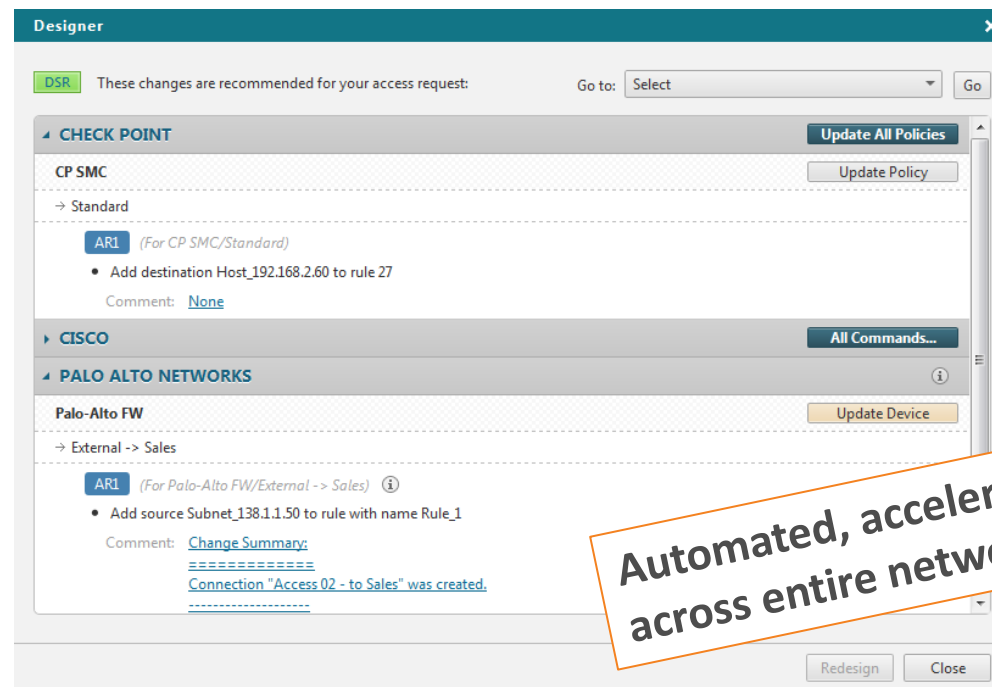
Automated change design based on accurate topology simulation & path analysis across vendors & platforms



# Automated, Accelerated Implementation



Automated provisioning for leading network security platforms  
reduces complexity & eliminates human error



Automated, accelerated provisioning  
across entire network via single console

# Auditable Change Process



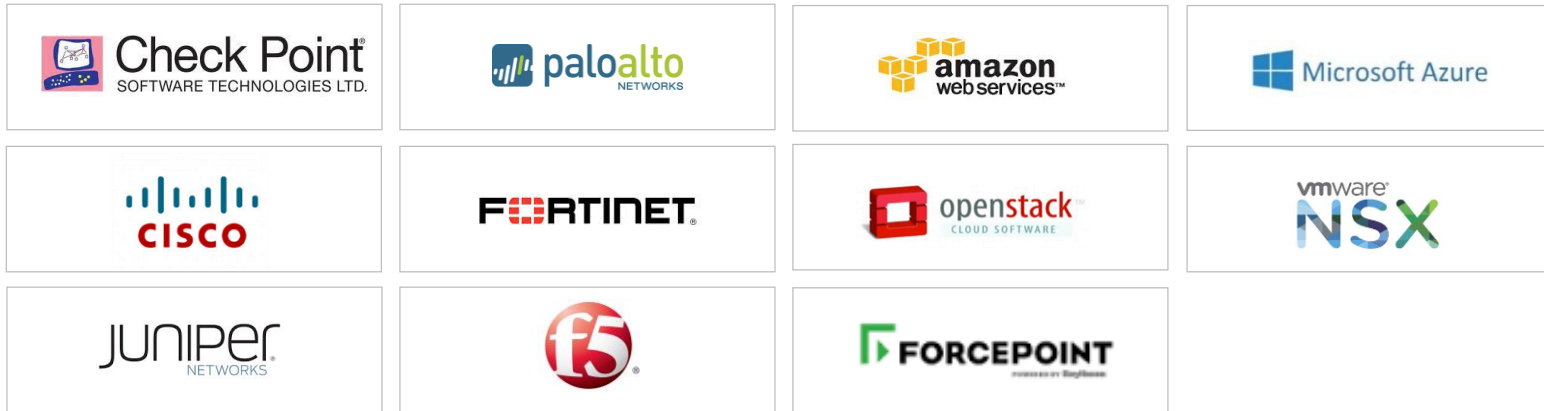
Ensure compliance by enforcing an auditable change process  
& addressing *ad hoc* changes & overly permissive access

Device	#	Changed on	Received on	Administrator	Action	Ticket ID	Authorized	Comment
Palo-Alto FW	82	14/01/16 15:31	14/01/16 15:32	admin (r)		93	Unauthorized	
Palo-Alto FW	81	14/01/16 15:28	14/01/16 15:28	admin (r)		94	Unauthorized	
Palo-Alto FW	80	14/01/16 15:10	14/01/16 15:10	-			Authorized	
Palo-Alto FW	79	14/01/16 15:07	14/01/16 15:08	admin (r)		93	Unauthorized	
Panorama	6	14/01/16 15:07	14/01/16 15:08	admin (r)		93	N/A	
Palo-Alto FW	78	10/01/16 17:00	10/01/16 17:00	-			Authorized	
Palo-Alto FW	77	10/01/16 16:00	10/01/16 16:00	-			Authorized	
Palo-Alto FW	76	06/01/16 17:00	06/01/16 17:00	-			Unauthorized	
ASAv	103	31/12/15 18:05	31/12/15 19:05	admin			Unauthorized	
PAN Cluster	21	31/12/15 19:00	31/12/15 19:00	-			Unauthorized	
ASAv	102	31/12/15 17:05	31/12/15 18:05	admin			Authorized	
PAN Cluster	20	31/12/15 18:00	31/12/15 18:00	-			Authorized	
Palo-Alto FW	75	29/12/15 12:00	29/12/15 12:00	-			Unauthorized	
ASAv	101	28/12/15 18:05	28/12/15 19:05	admin			Unauthorized	
PAN Cluster	19	28/12/15 19:00	28/12/15 19:00	-			Unauthorized	
ASAv	100	28/12/15 10:05	28/12/15 11:05	admin			Authorized	

Full accountability with  
automatic audit trail of all  
network security changes  
✓ Authorized  
Unauthorized

# Technology Partners & Integrations

## Network & Cloud Platforms



## IT Service Management



# Summary

**Tufin makes security manageable across hybrid networks  
with network security policy orchestration**

**Maximize Agility & Security**



**Ensure Continuous Compliance**



**Gain Visibility & Control**





Thank You!