Présentation Tufin Security Suite

Frédéric Nakhlé
frederic@tufin.com
06 70 16 15 53

Jean-Michel Tavernier
Jean-michel@tufin.com
06 04 11 11 06

Tufin

- Tufin est une société créée en 2005, 200 personnes dans le monde
- 1300 clients grand-compte dans le monde et plus de 80 références en France
- Partenaires technologiques:

Check Point SOFTWARE TECHNOLOGIES LTD

FORTINET

CISCO

Blue Coat

paloalto NETWORKS

Juniper NETWORKS

McAfee Proven Security

f5 NETWORKS

bmcsoftware

Challenges du Management IT

Complexité

- Les enterprises ont des centaines de firewalls, routeurs et switchs
- Chaque équipement peut avoir des règles extrèmement complexes, plus de 100

Changement Constant

Les grandes entreprises ou institutions on entre 10 à 100 changements par semaine

Connectivité

Une erreur de configuration peut engendrer la perte d’accès aux applications.

Compliance

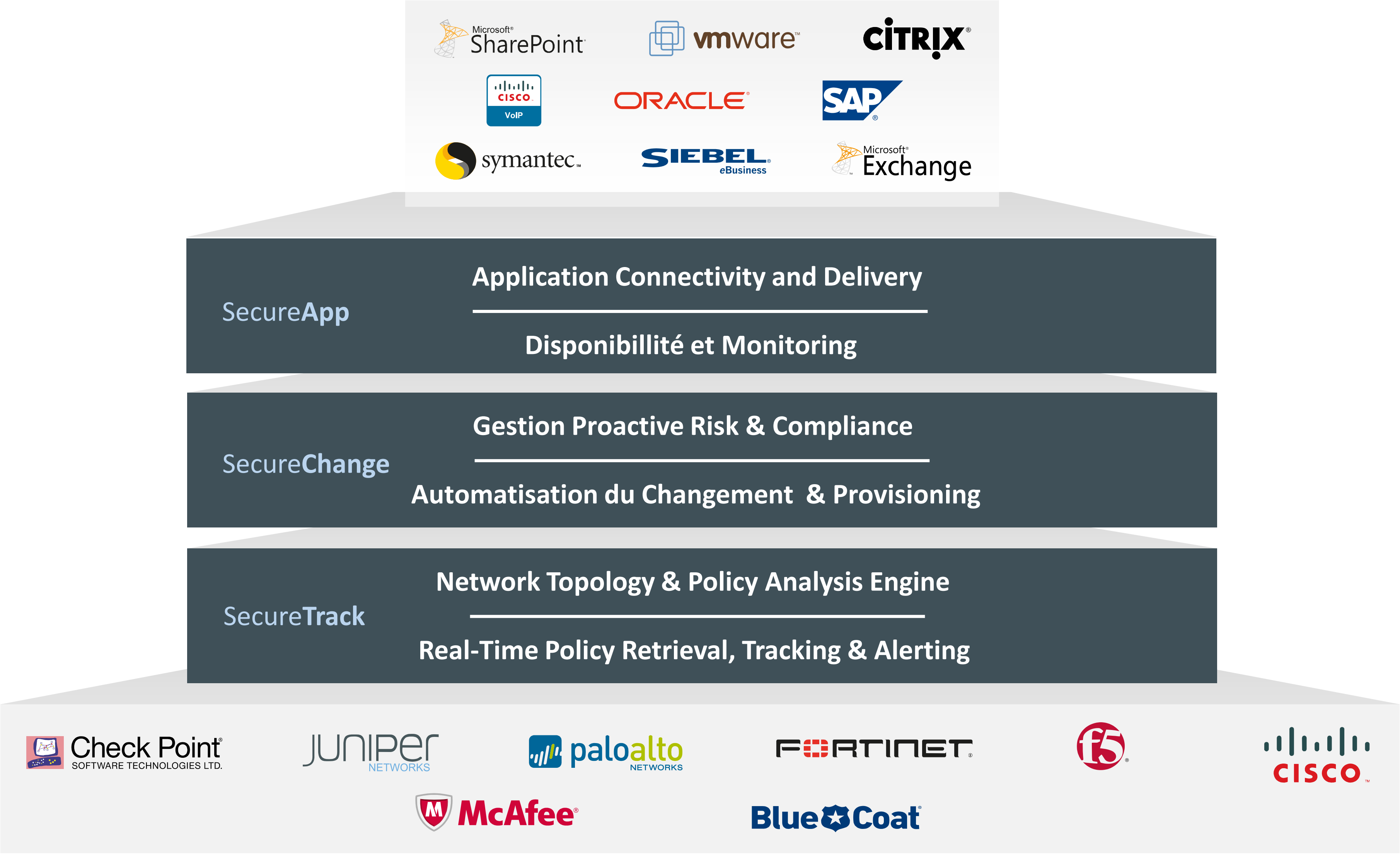
- Le nombre de standard ne cesse d’augmenter: PCI-DSS, SOX, NERC, etc…
- La preparation d’une audit est très chronofage et monopolise de nombreuses ressources

Communication

- La plus part des changements sont liés a des applications
- La communication reste difficile entre les personnes en charges des applications et les équipes réseaux, sécu

Bottom line: firewall changes take 1-2 weeks to implement

La solution Tufin



SecureApp

Application Connectivity and Delivery

Disponibillité et Monitoring

SecureChange

Gestion Proactive Risk & Compliance

Automatisation du Changement & Provisioning

SecureTrack

Network Topology & Policy Analysis Engine

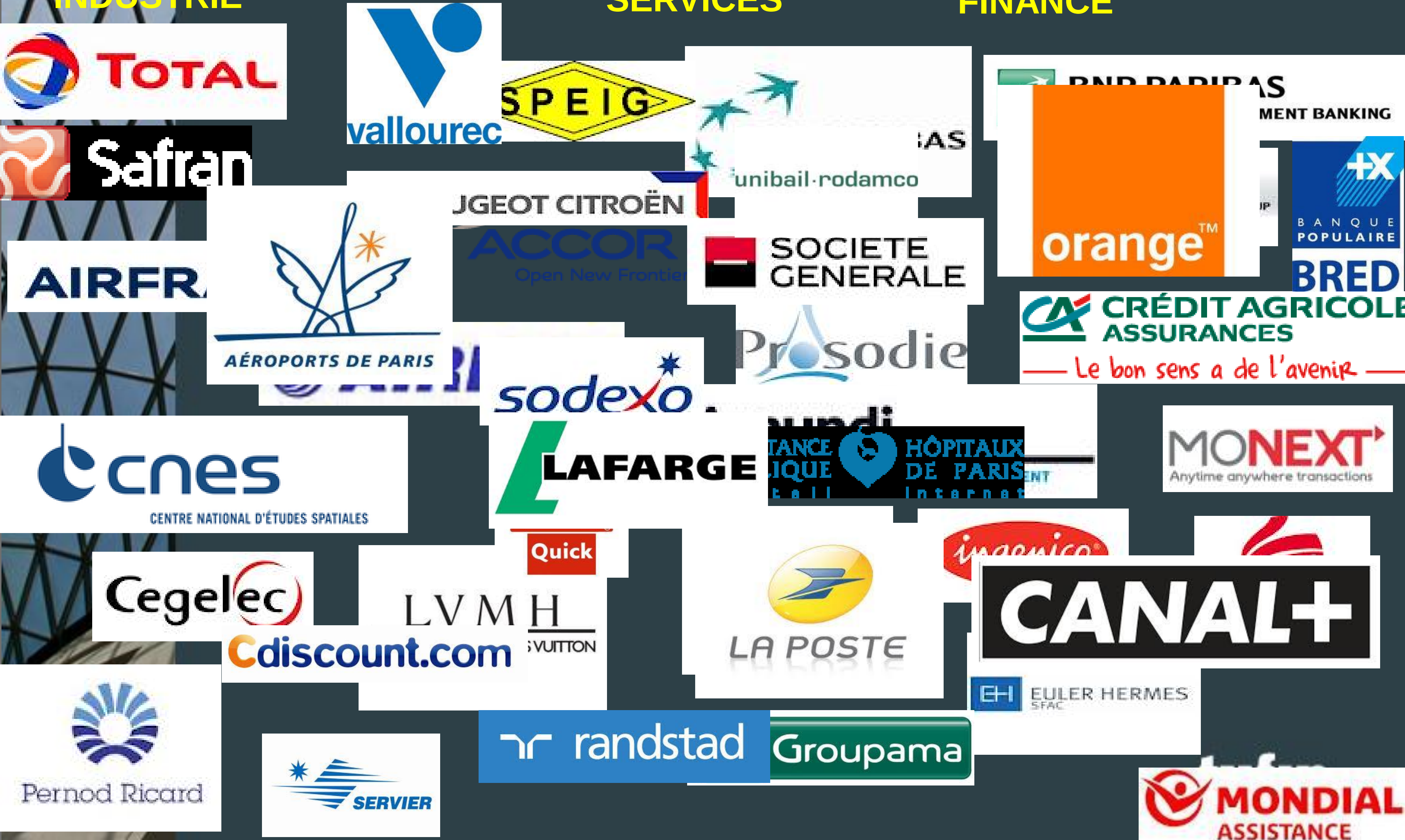
Real-Time Policy Retrieval, Tracking & Alerting

Quelques Clients Français

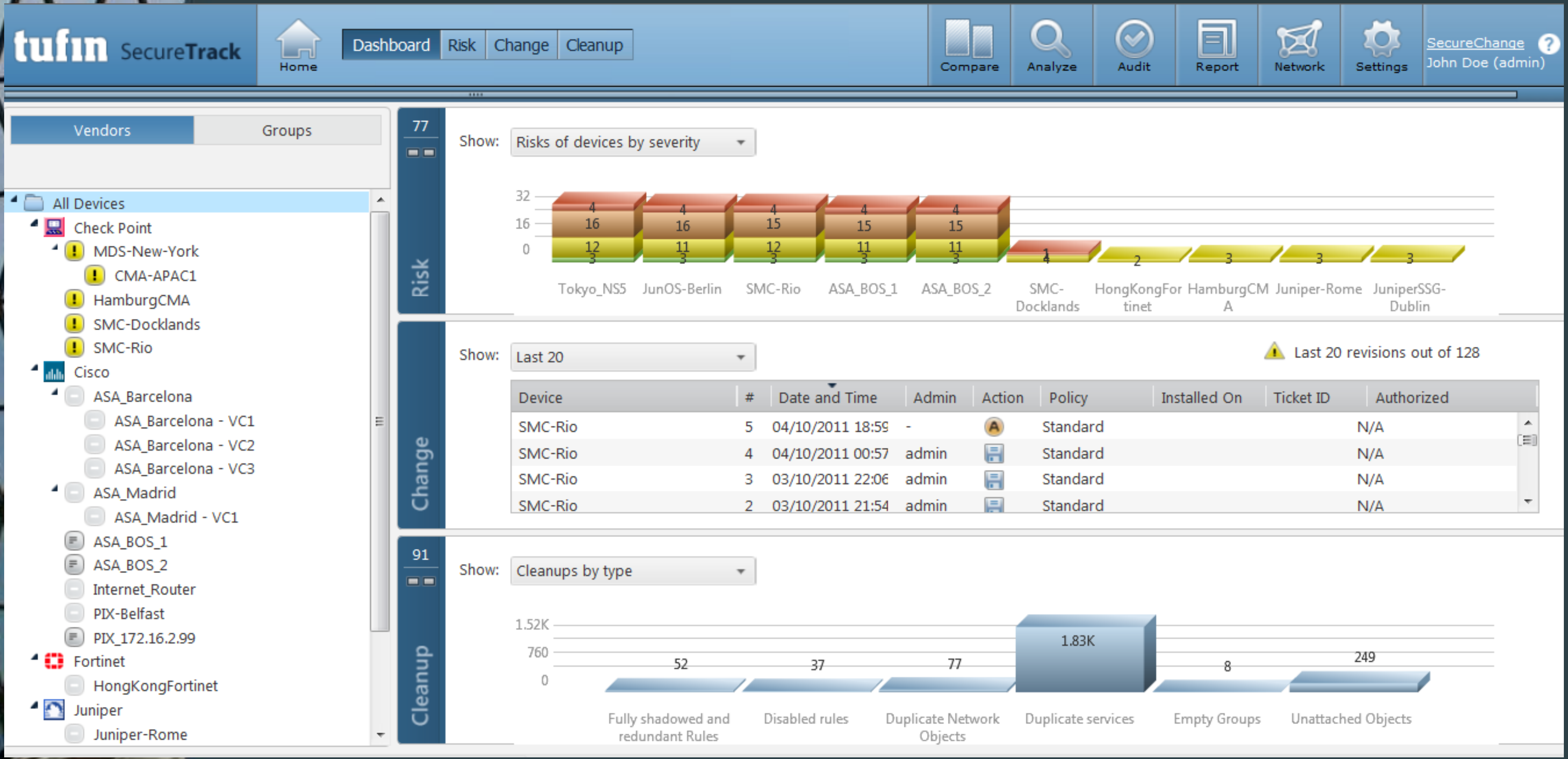
INDUSTRIE

SERVICES

FINANCE



Point fort de la solution SecureTrack: Dashboard



Show: Risks of devices by severity

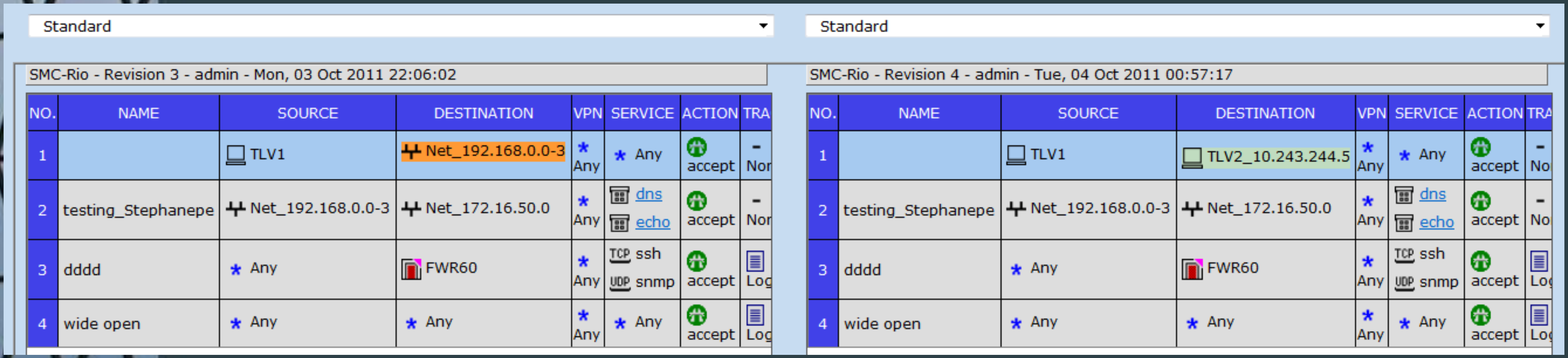
Show: Last 20

⚠ Last 20 revisions out of 128

Device	#	Date and Time	Admin	Action	Policy	Installed On	Ticket ID	Authorized
SMC-Rio	5	04/10/2011 18:59	-	Ⓐ	Standard			N/A
SMC-Rio	4	04/10/2011 00:57	admin	🖫	Standard			N/A
SMC-Rio	3	03/10/2011 22:06	admin	🖫	Standard			N/A
SMC-Rio	2	03/10/2011 21:54	admin	🖫	Standard			N/A

Show: Cleanups by type

Point fort de la solution: Compare Revisions



Standard

SMC-Rio - Revision 3 - admin - Mon, 03 Oct 2011 22:06:02

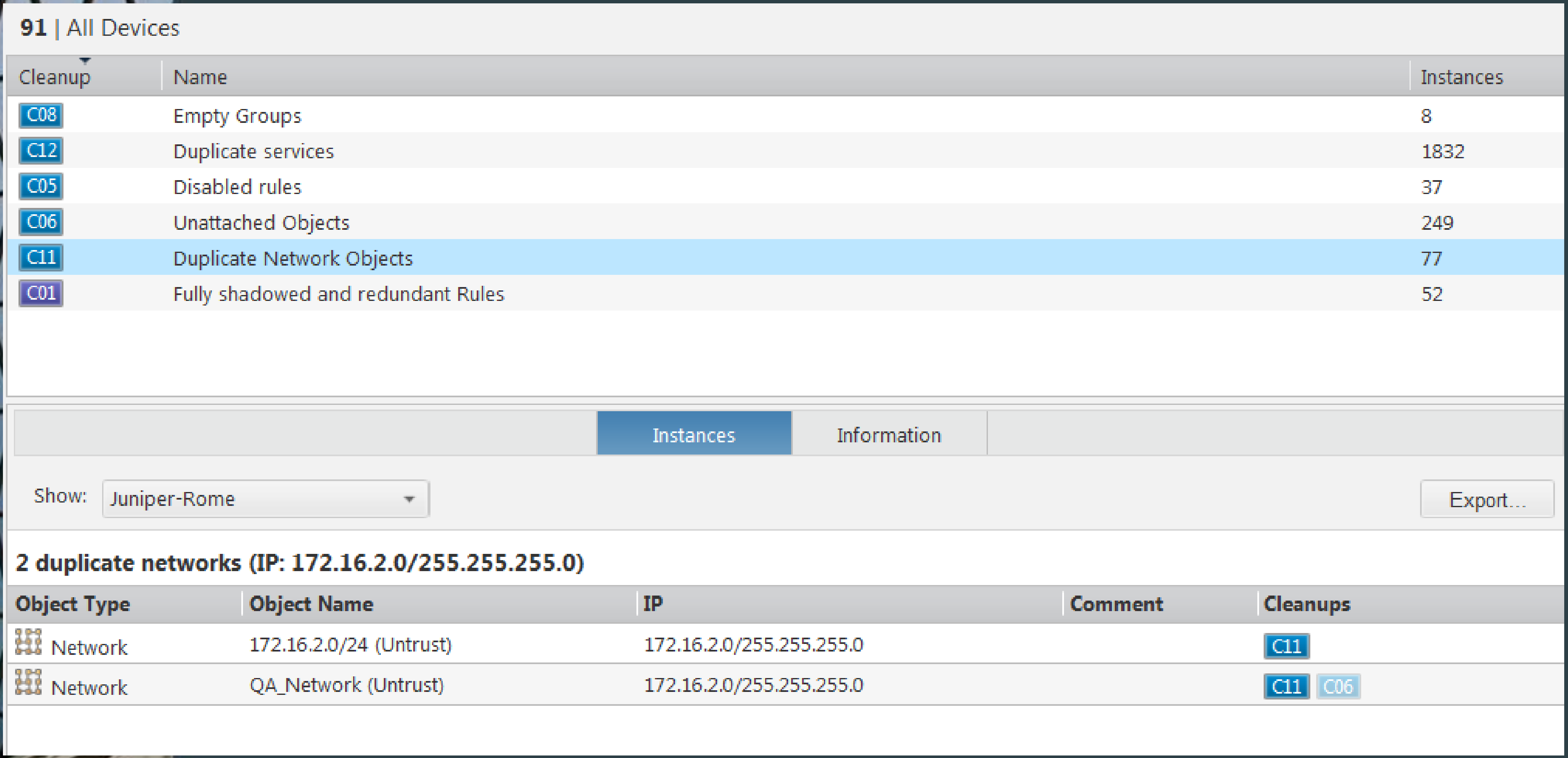
NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRA
1		TLV1	Net_192.168.0.0-3	* Any	* Any	accept	- Nor
2	testing_Stephanepe	Net_192.168.0.0-3	Net_172.16.50.0	* Any	dns echo	accept	- Nor
3	dddd	* Any	FWR60	* Any	TCP ssh UDP snmp	accept	Log
4	wide open	* Any	* Any	* Any	* Any	accept	Log

Standard

SMC-Rio - Revision 4 - admin - Tue, 04 Oct 2011 00:57:17

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRA
1		TLV1	TLV2_10.243.244.5	* Any	* Any	accept	- No
2	testing_Stephanepe	Net_192.168.0.0-3	Net_172.16.50.0	* Any	dns echo	accept	- No
3	dddd	* Any	FWR60	* Any	TCP ssh UDP snmp	accept	Lo
4	wide open	* Any	* Any	* Any	* Any	accept	Lo

Point fort de Securetrack: Le Cleanup



91 | All Devices

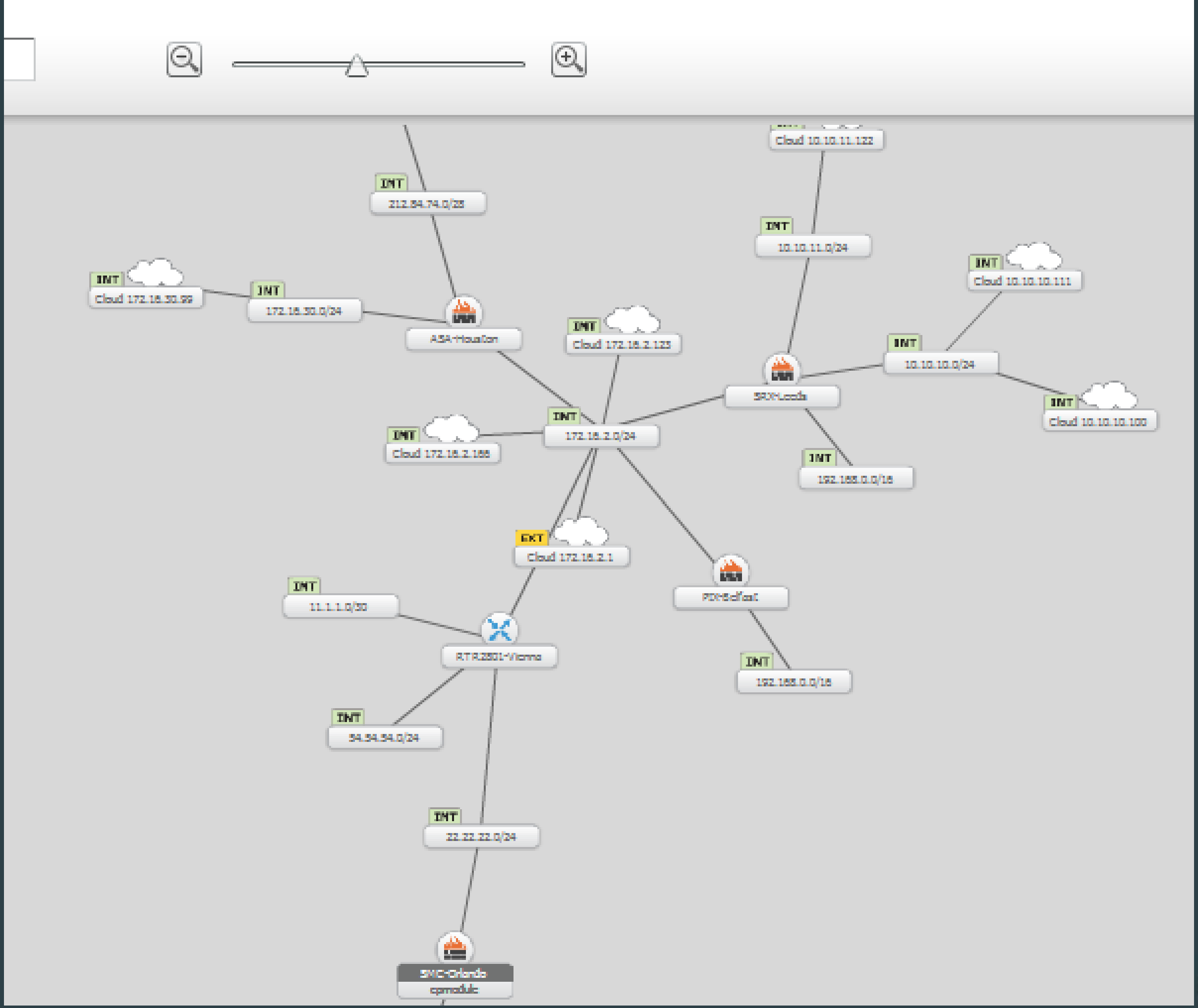
Cleanup	Name	Instances
C08	Empty Groups	8
C12	Duplicate services	1832
C05	Disabled rules	37
C06	Unattached Objects	249
C11	Duplicate Network Objects	77
C01	Fully shadowed and redundant Rules	52

Show: Juniper-Rome

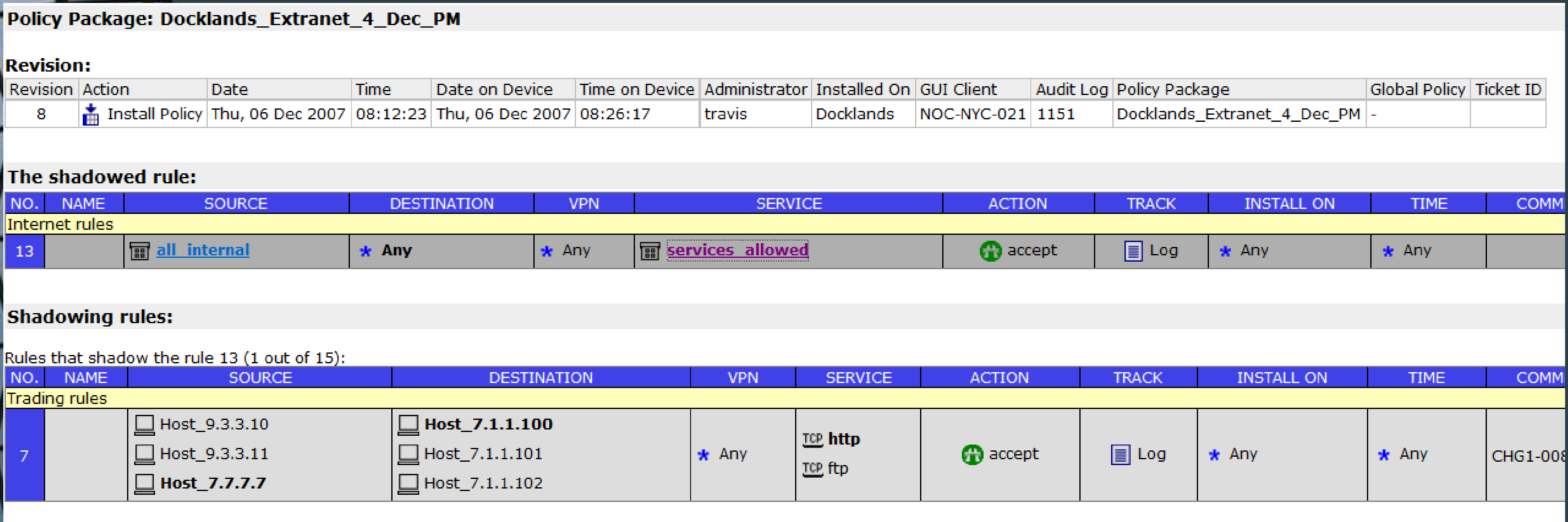
2 duplicate networks (IP: 172.16.2.0/255.255.255.0)

Object Type	Object Name	IP	Comment	Cleanups
Network	172.16.2.0/24 (Untrust)	172.16.2.0/255.255.255.0		C11
Network	QA_Network (Untrust)	172.16.2.0/255.255.255.0		C11 C06

Point fort SecureTrack: La Topologie



Point fort SecureTrack: Rules Analysis



Policy Package: Docklands_Extranet_4_Dec_PM

Revision:

Revision	Action	Date	Time	Date on Device	Time on Device	Administrator	Installed On	GUI Client	Audit Log	Policy Package	Global Policy	Ticket ID
8	Install Policy	Thu, 06 Dec 2007	08:12:23	Thu, 06 Dec 2007	08:26:17	travis	Docklands	NOC-NYC-021	1151	Docklands_Extranet_4_Dec_PM	-	

The shadowed rule:

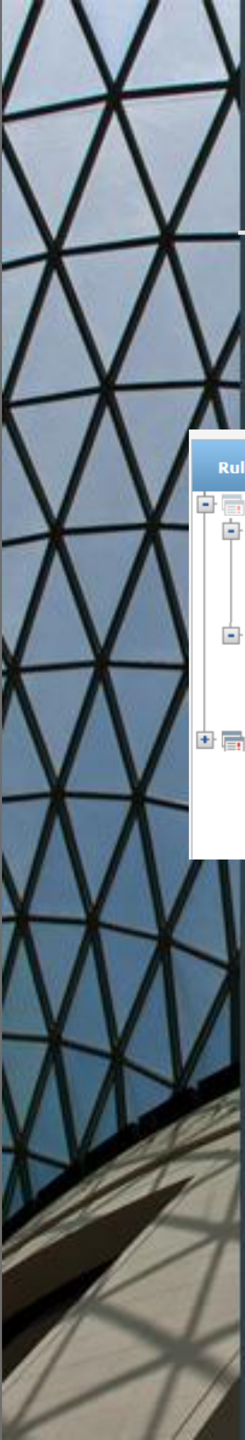
NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMM
Internet rules										
13		all_internal	* **Any**	* Any	services_allowed	accept	Log	* Any	* Any	

Shadowing rules:

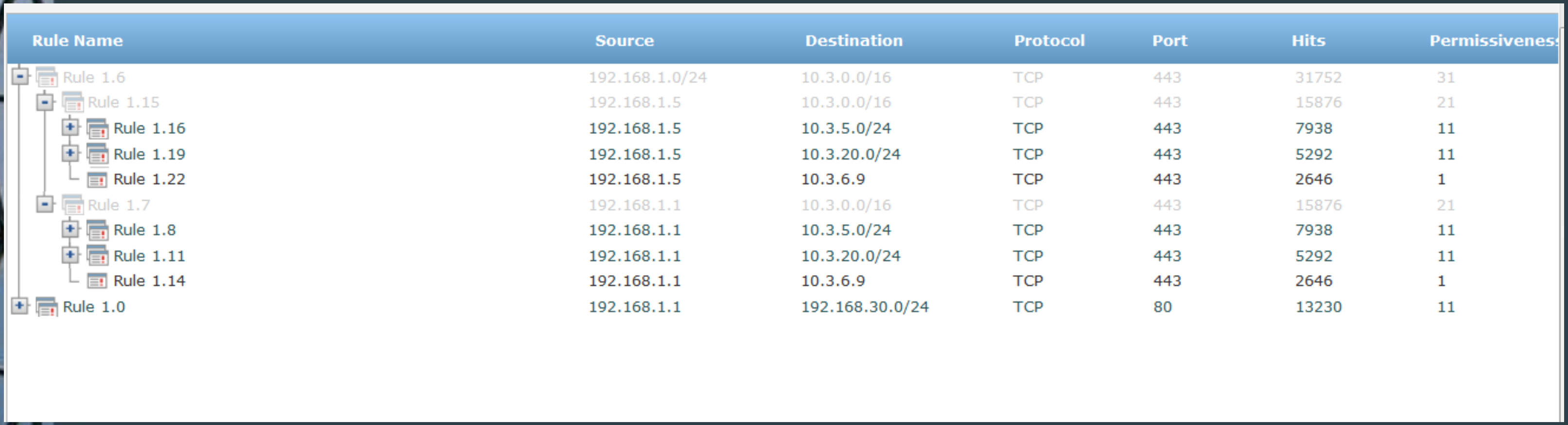
Rules that shadow the rule 13 (1 out of 15):

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMM
Trading rules										
7		Host_9.3.3.10 Host_9.3.3.11 **Host_7.7.7.7**	**Host_7.1.1.100** Host_7.1.1.101 Host_7.1.1.102	* Any	TCP **http** TCP ftp	accept	Log	* Any	* Any	CHG1-008

tufin



Point fort SecureTrack: APG

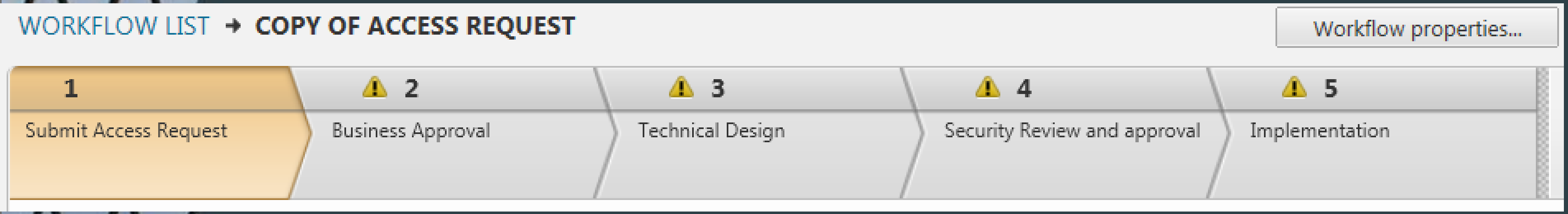


Rule Name	Source	Destination	Protocol	Port	Hits	Permissivenes
Rule 1.6	192.168.1.0/24	10.3.0.0/16	TCP	443	31752	31
Rule 1.15	192.168.1.5	10.3.0.0/16	TCP	443	15876	21
Rule 1.16	192.168.1.5	10.3.5.0/24	TCP	443	7938	11
Rule 1.19	192.168.1.5	10.3.20.0/24	TCP	443	5292	11
Rule 1.22	192.168.1.5	10.3.6.9	TCP	443	2646	1
Rule 1.7	192.168.1.1	10.3.0.0/16	TCP	443	15876	21
Rule 1.8	192.168.1.1	10.3.5.0/24	TCP	443	7938	11
Rule 1.11	192.168.1.1	10.3.20.0/24	TCP	443	5292	11
Rule 1.14	192.168.1.1	10.3.6.9	TCP	443	2646	1
Rule 1.0	192.168.1.1	192.168.30.0/24	TCP	80	13230	11

Point fort: SecureChange

- Workflow puissant
- Proposition de changements
- Aide à la décision
- Provisionning du changement
- Validation des Risks

Point fort SecureChange :Un workflow puissant



WORKFLOW LIST → COPY OF ACCESS REQUEST

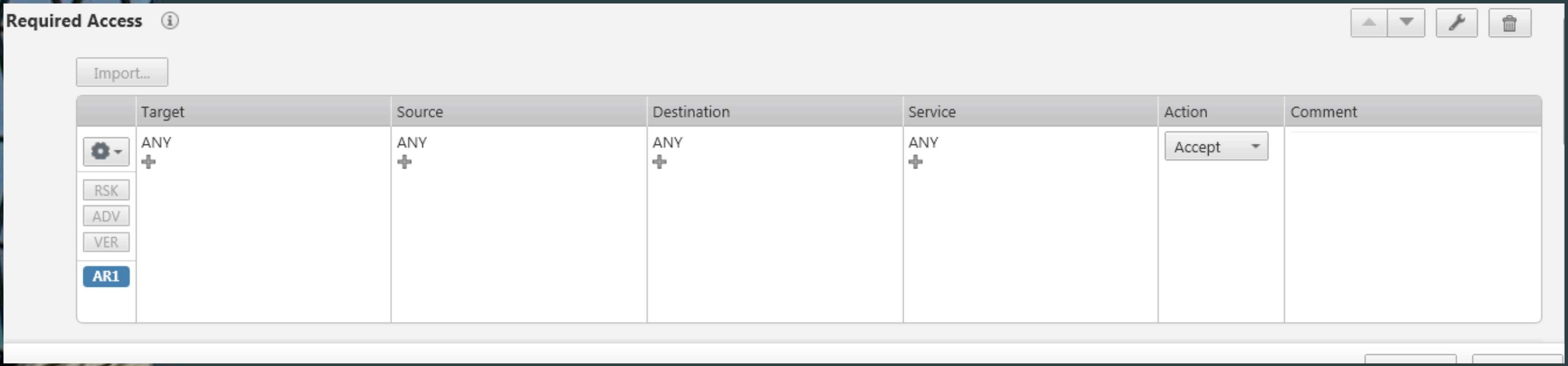
1 Submit Access Request

⚠ 2 Business Approval

⚠ 3 Technical Design

⚠ 4 Security Review and approval

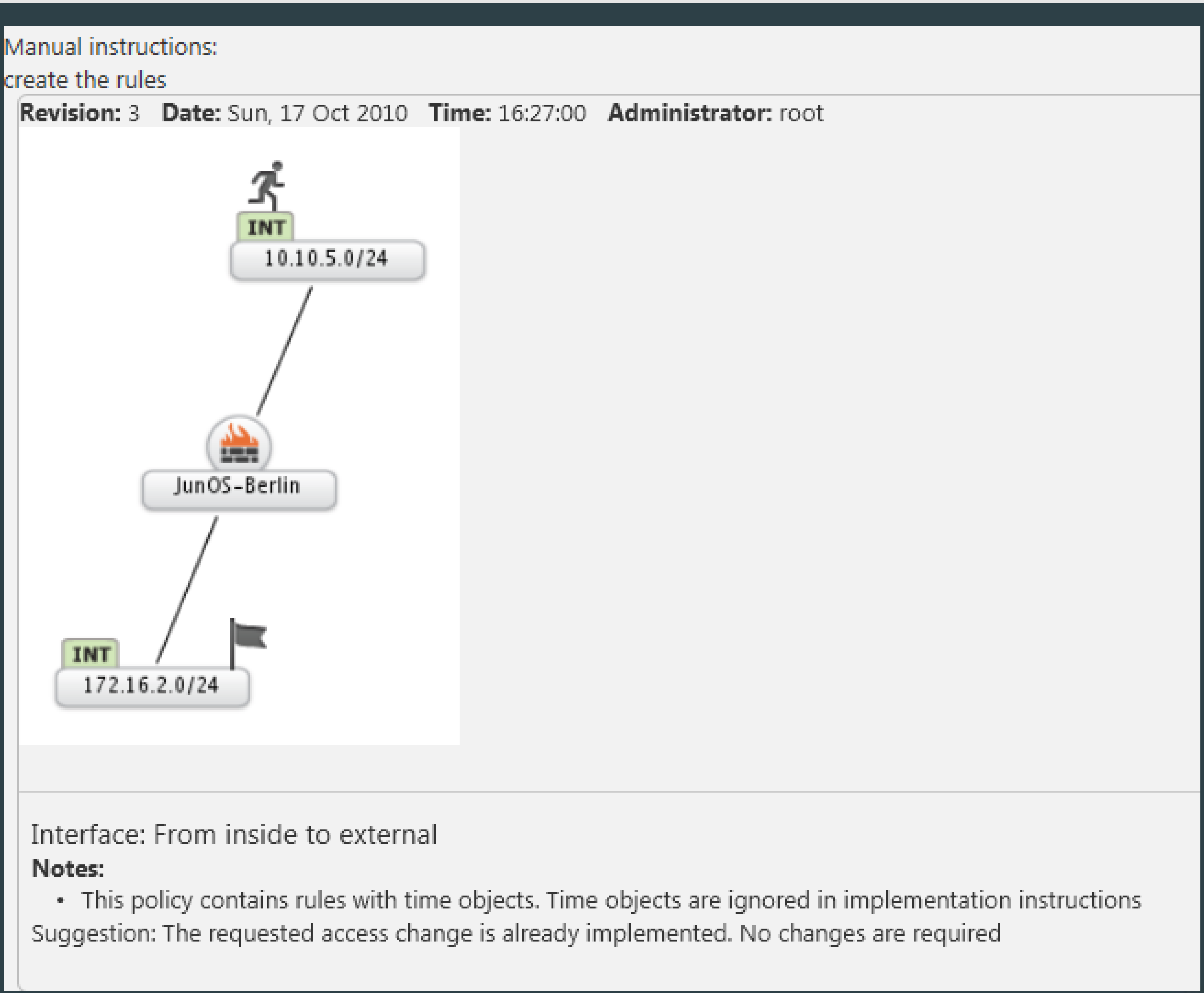
⚠ 5 Implementation



Required Access

	Target	Source	Destination	Service	Action	Comment
AR1	ANY	ANY	ANY	ANY	Accept	

Point Fort : Propositions de changements



Manual instructions:
create the rules

Revision: 3 **Date:** Sun, 17 Oct 2010 **Time:** 16:27:00 **Administrator:** root

Interface: From inside to external

Notes:

- This policy contains rules with time objects. Time objects are ignored in implementation instructions

Suggestion: The requested access change is already implemented. No changes are required

Point Fort SecureChange: Risk et API

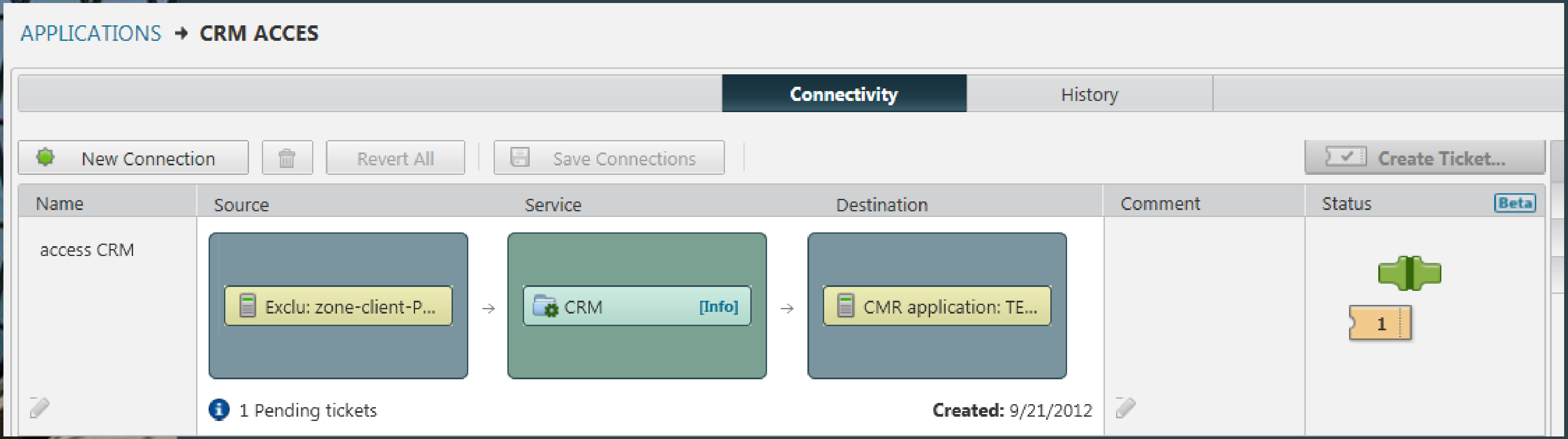
- Validation des RISK
- En fonction des règles de compliances définies sur SecureTrack
- Possibilité d’autoriser un risque manuellement

- API pour implementation dans votre Ticketing Tools

tufin

SecureAPP

- Solution pour les applications owner
  - Orienté application
  - Permettant de publier des applications rapidement
  - Orienté Application Owner
  - Plus de connaissance reseau necessaire.



Name	Source	Service	Destination	Comment	Status
access CRM	Exclu: zone-client-P... →	CRM [Info] →	CMR application: TE...		1

1 Pending tickets

Created: 9/21/2012

Merci

www.tufin.com