Tufin Orchestration Suite:
целевой контроль логического доступа в сети

Структура презентации

- ✓ Профиль действующих клиентов в России
- ✓ Ключевые блоки функционала решения
- ✓ Топологический анализ данных
- ✓ История изменений доступов
- ✓ Оптимизация конфигураций устройств
- ✓ Преимущества решения Tufin

tufin

Профиль клиентов в России:

✓ **ФИНАНСОВЫЙ СЕКТОР**

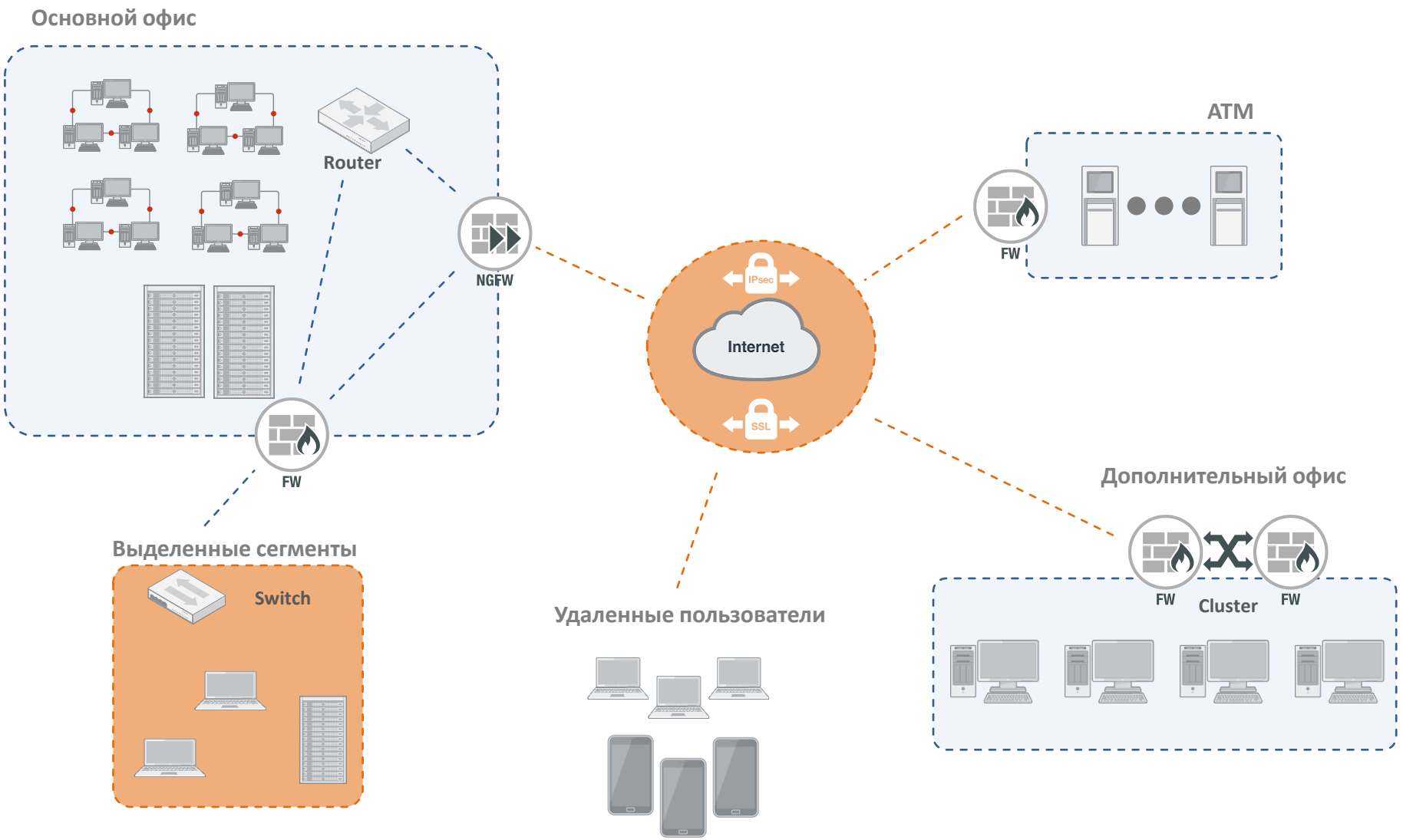
✓ **НЕФТЕГАЗОВЫЙ СЕКТОР**

✓ **ТЕЛЕКОММУНИКАЦИИ**

✓ **ПРОМЫШЛЕННОСТЬ И ДР.**

NETWELL

Система контроля и управления логическим доступом:
от простой до сложной сети



Ключевой пул поддерживаемых решений (примеры)

- ✓ Поддержка консолей управления и отдельных устройств от ведущих вендоров: Palo Alto (PA – Services/Users), Fortinet, Cisco, McAfee, Stonesoft, Forcepoint, Checkpoint, BlueCoat, Juniper, F5 BIG IP и другие…
- ✓ Все, что Linux на основе Red Hat - IPTables
- ✓ Коммутаторы, NLB, Generic Type

NETWELL

Ключевые блоки функционала Tufin TOS:

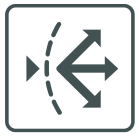
работа с сетевым оборудованием

Интерактивная сетевая карта

Анализ изменений в реальном времени

Единая точка внесения изменений

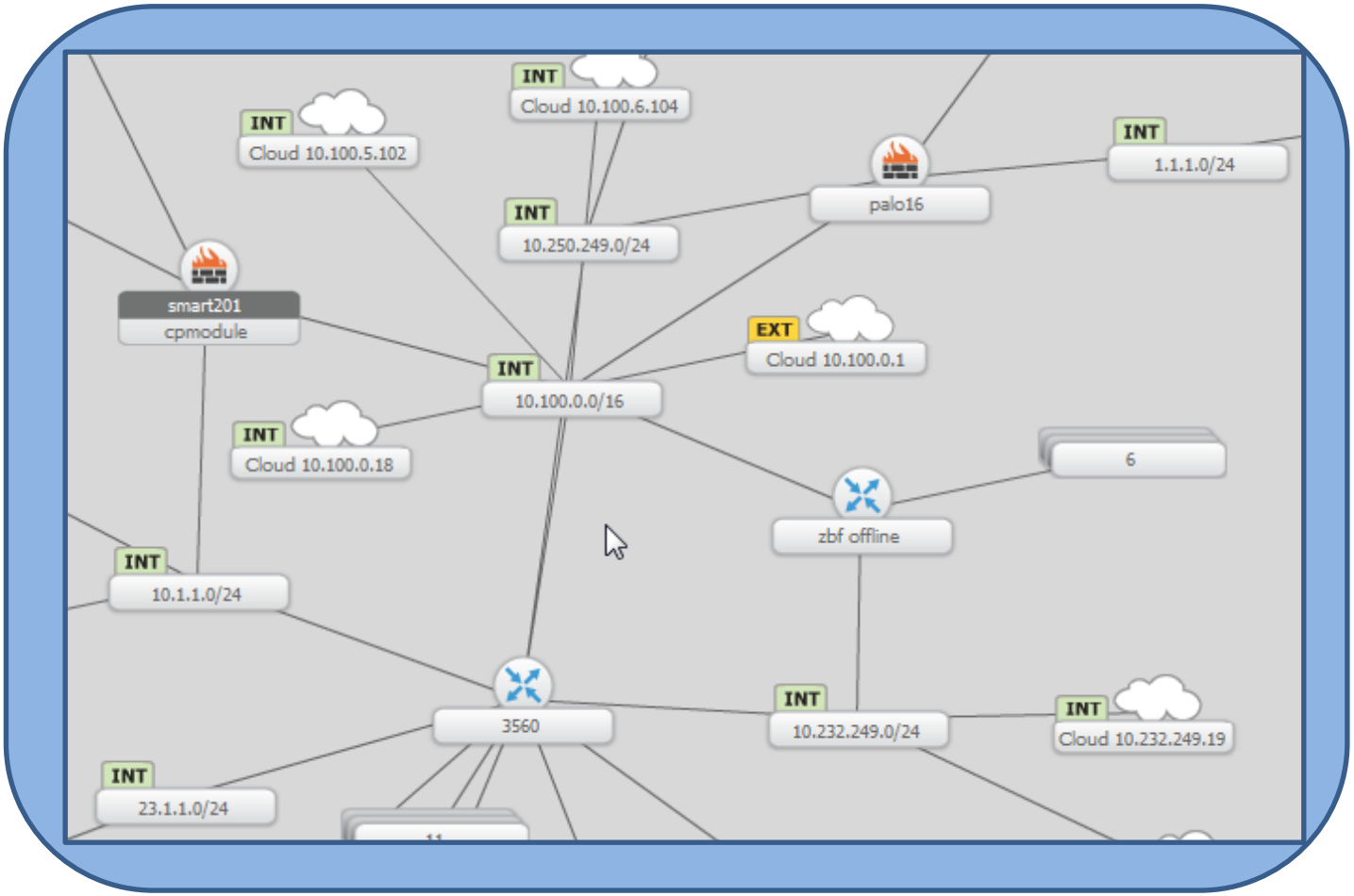
Оптимизация баз правил



Распределение ответственности

Риски и оценка безопасности

Сетевая топологическая карта



✓ **Учитываем маршрутизацию, VPN, VRF, MPLS, NAT и т.д.**

Контроль логического доступа по всей сети

Каким образом это делаем с решением от Tufin?

- Знаем архитектуру, синтаксис и строение ACL оборудования
- Понимаем уровень объектов (сервис, хост, группа)
- Смотрим, какой трафик действительно есть

5	✓	1.1.1.5	NewDest	OSPF	inside	in	asdasd	
6	✓	25.0.2.0/24	24.0.2.0/24	icmp/0/1	inside	in	zorik test1	
7	✓	All-IPv4-Addresses	192.168.120.98	TFTP-UDP	inside	in	sds	

4		LAN2_172.16.2.0	sky_192.168.3.70	* Any	TCP http TCP ftp TCP https	Accept	Log	* Any	* Any

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Options	Comment
1	Oracle_36	z1	z1	Dev_IP_Range	Any	Orace_server_36-1	oracle	application-default	✓		Access of Dev to Oracle
2	CRM_47	z1	z1	Dev_IP_Range	Any	CRM_Server_47-1	siebel-crm salesforce	application-default	✓		Access from DEV to the CRM on 47
3	Block_Critical_Apps	any	z1	DMZ	Any	Orace_server_36-1 CRM_Server_47-1	Any	Any	✗		Protect Oracle and CRM

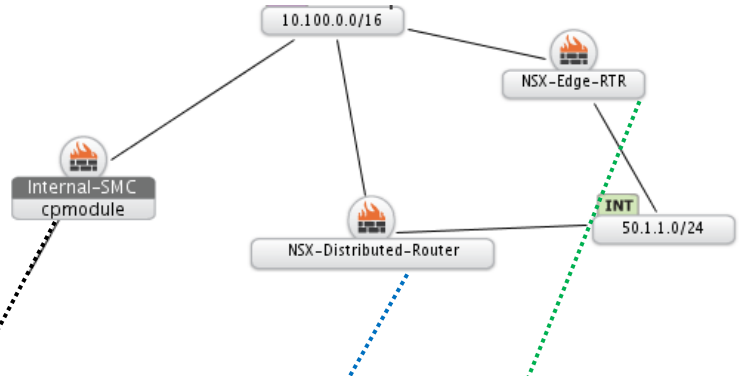
Сервис

Хост

Приложение

Контроль логического доступа по всей сети

По всем возможным путям прохождения трафика получаем отчет только о релевантных правилах доступа



Такого доступа не будет, сработает правило № 362

* Any	* Any	* Any	* Any	drop	– None	* Any	* Any

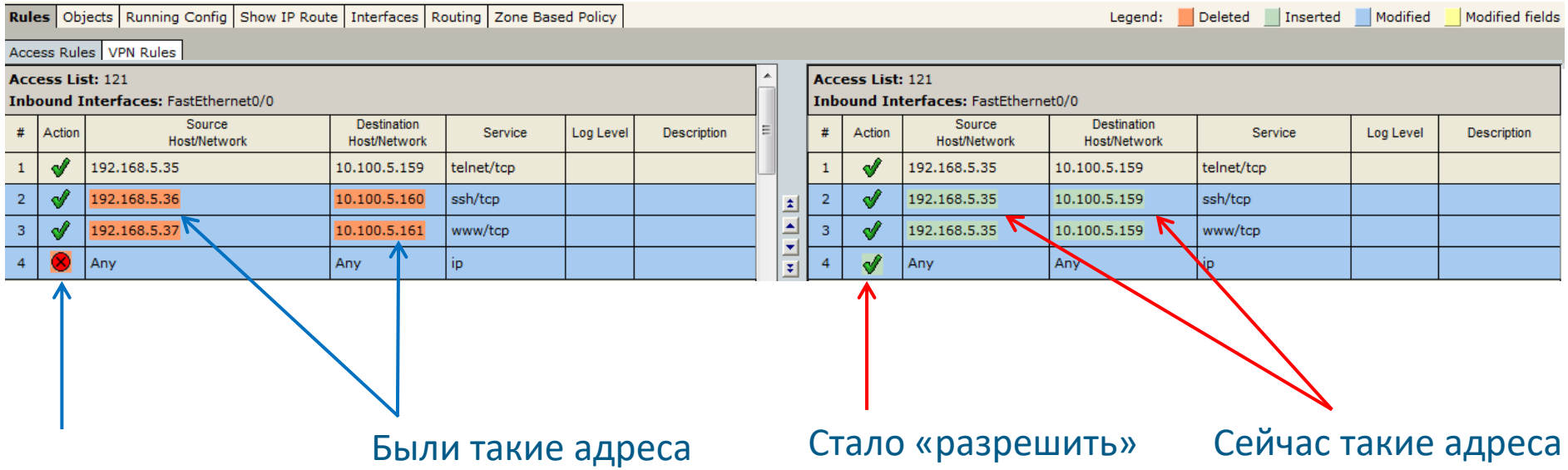
Сработает правило № 13, «пройдем»

13		Web01 - Network adapter 2 ipset_range test_icon MGMT-PortGroup		DC_test2 MGMT MGMT-PortGroup none		Data Recovery Appliance DNS UDP_500	

Такого доступа не будет, сработает правило № 53

53	Partially Shadowed Details...	Default Rule	* Any		* Any	* Any

Анализ изменений в реальном времени (и история)



Были такие адреса

Стало «разрешить»

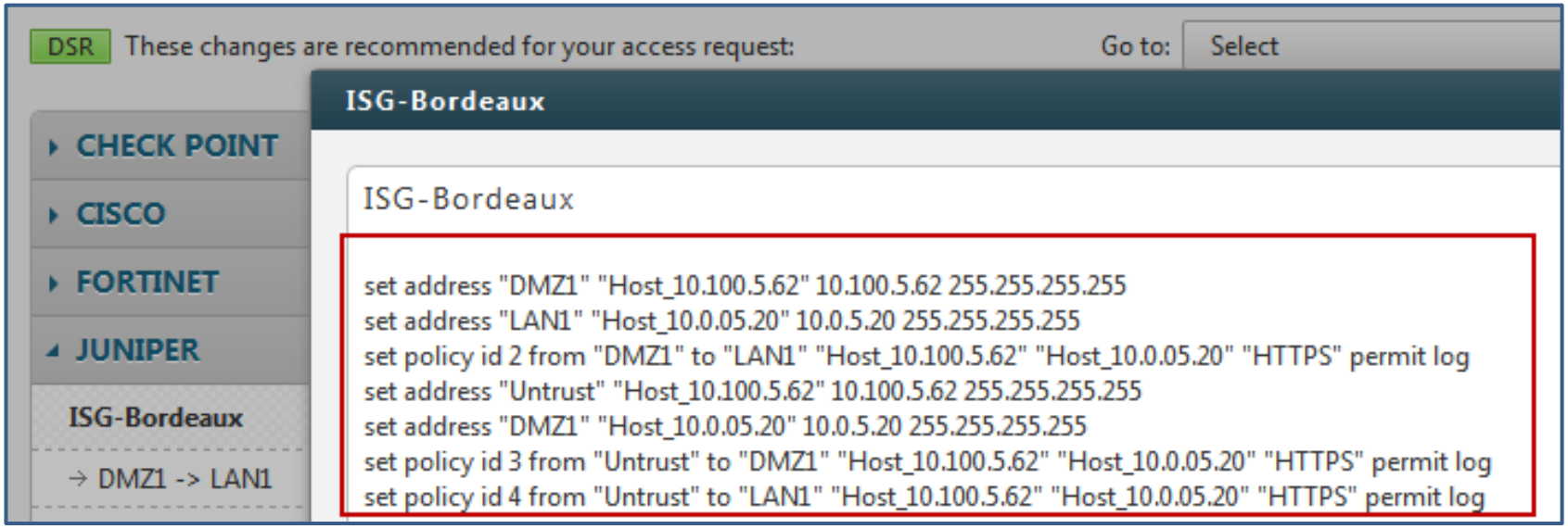
Сейчас такие адреса

Пару минут назад в правилах 2, 3 и 4

Сейчас в правилах 2, 3 и 4

tufin

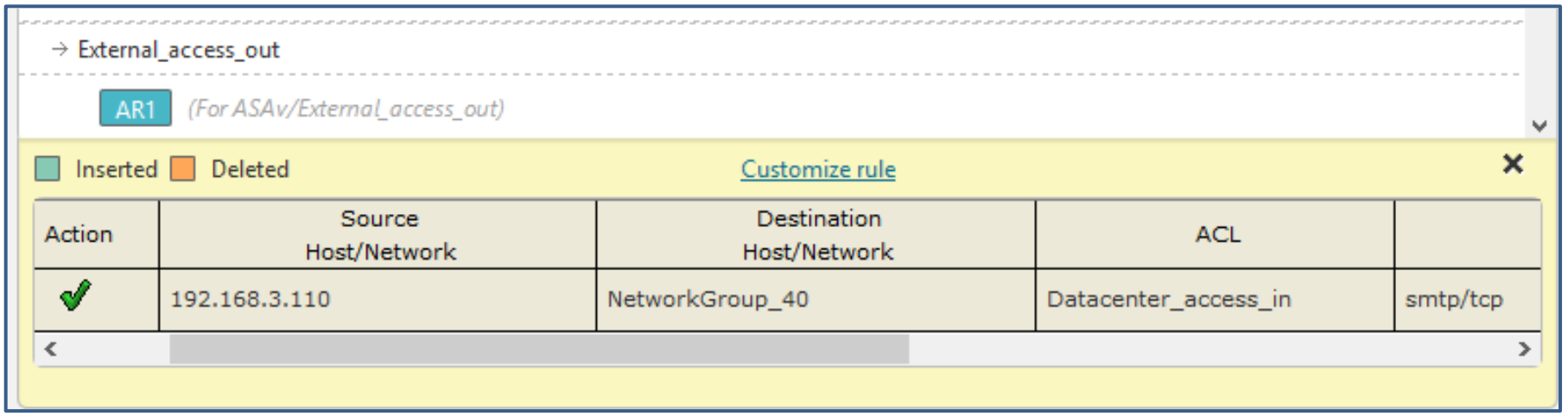
Единая контролируемая точка внесения изменений



- ✓ Автоматическое написание и **ВНЕДРЕНИЕ** требуемого правила
- ✓ Для оборудования **Palo Alto, Fortinet, Checkpoint, Cisco, Juniper, Forcepoint (ex.Stonesoft)**
- ✓ Выбирается самый оптимальный способ

NETWELL

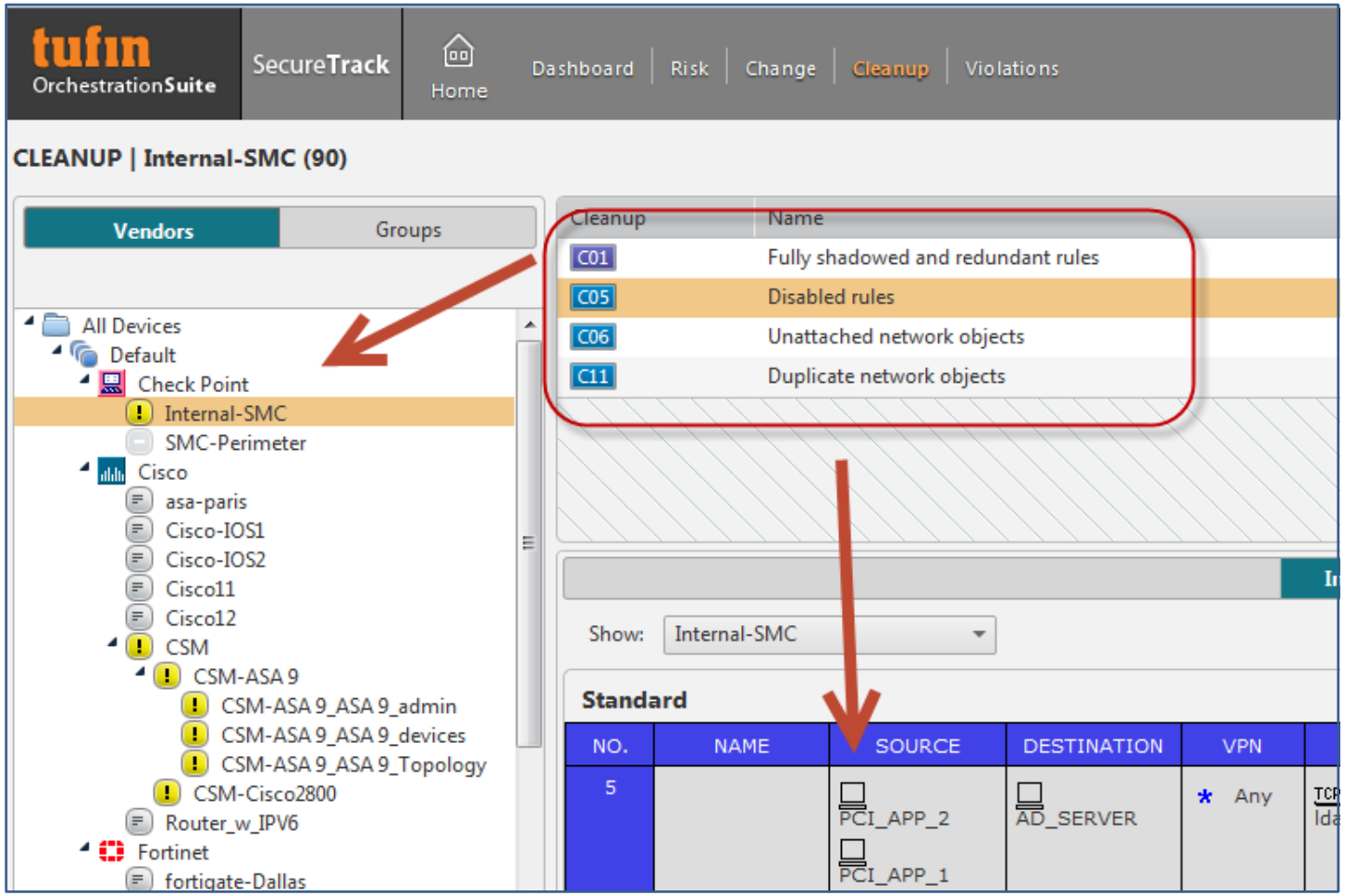
Единая контролируемая точка внесения изменений



- ✓ Какое правило будет: языком ОС и графическим представлением
- ✓ Сообразно «родным» интерфейсам производителей
- ✓ Прописывание правил автоматически, или после утверждения

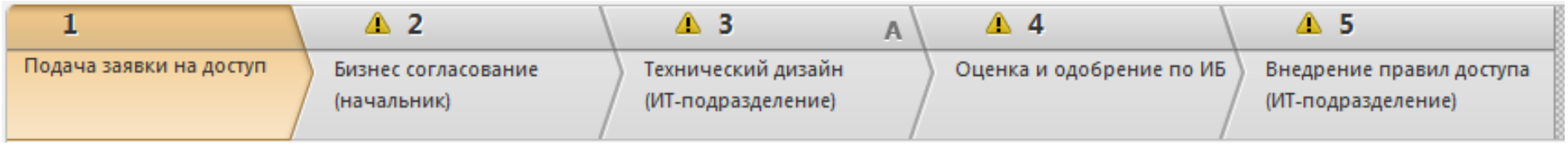
Оптимизация баз правил

- Частично и полностью «перекрывающиеся» правила
- Дублированные сервисы, хосты, группы и др. объекты
- «Отключенные» от правил объекты и др.



Распределение ответственности (бизнес-процессы)

Каждый отвечает за свой объем задач



- ✓ Разные системы имеют разную степень «критичности» - разные процедуры (workflow) и число участников
- ✓ Для каждого участника – «на своем языке»
- ✓ Привязка к оценке рисков и дизайну самих правил

tufin

Преимущества решения Tufin в данном секторе

- ✓ Получение изменений в режиме онлайн
- ✓ Лицензии мульти-вендорные и перемещаемые
- ✓ Конструктор заявок в GUI (не скрипты и Professional Service)
- ✓ Акцент в развитии решения – на автоматизацию доступов
- ✓ Есть поддержка offline-анализа

tufin

СПАСИБО ВАМ!