



tufin

Making Security Manageable

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

Профиль клиентов в России:



✓ **ФИНАНСОВЫЙ СЕКТОР**



✓ **НЕФТЕГАЗОВЫЙ СЕКТОР**

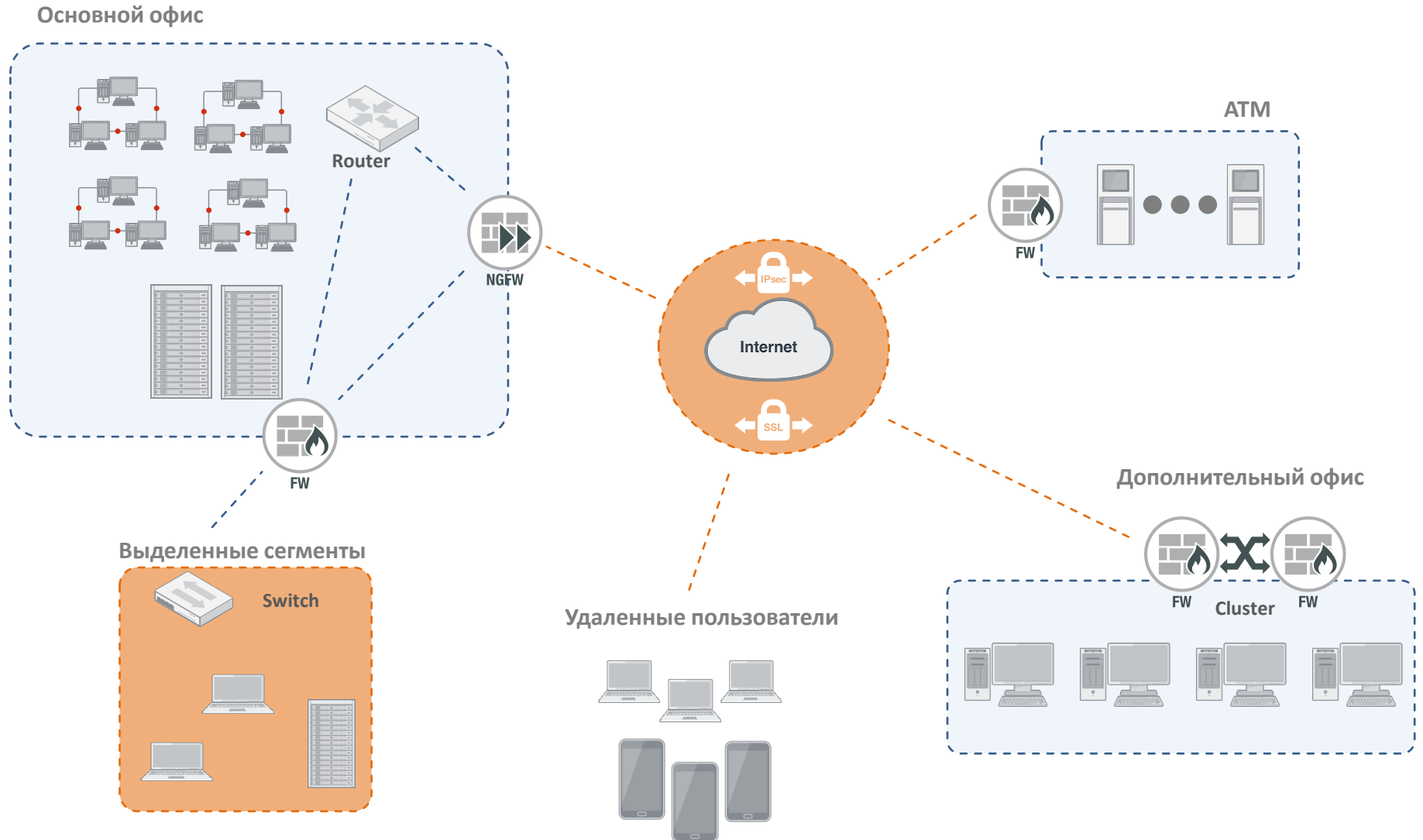


✓ **ТЕЛЕКОММУНИКАЦИИ**



✓ **ПРОМЫШЛЕННОСТЬ И ДР.**

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

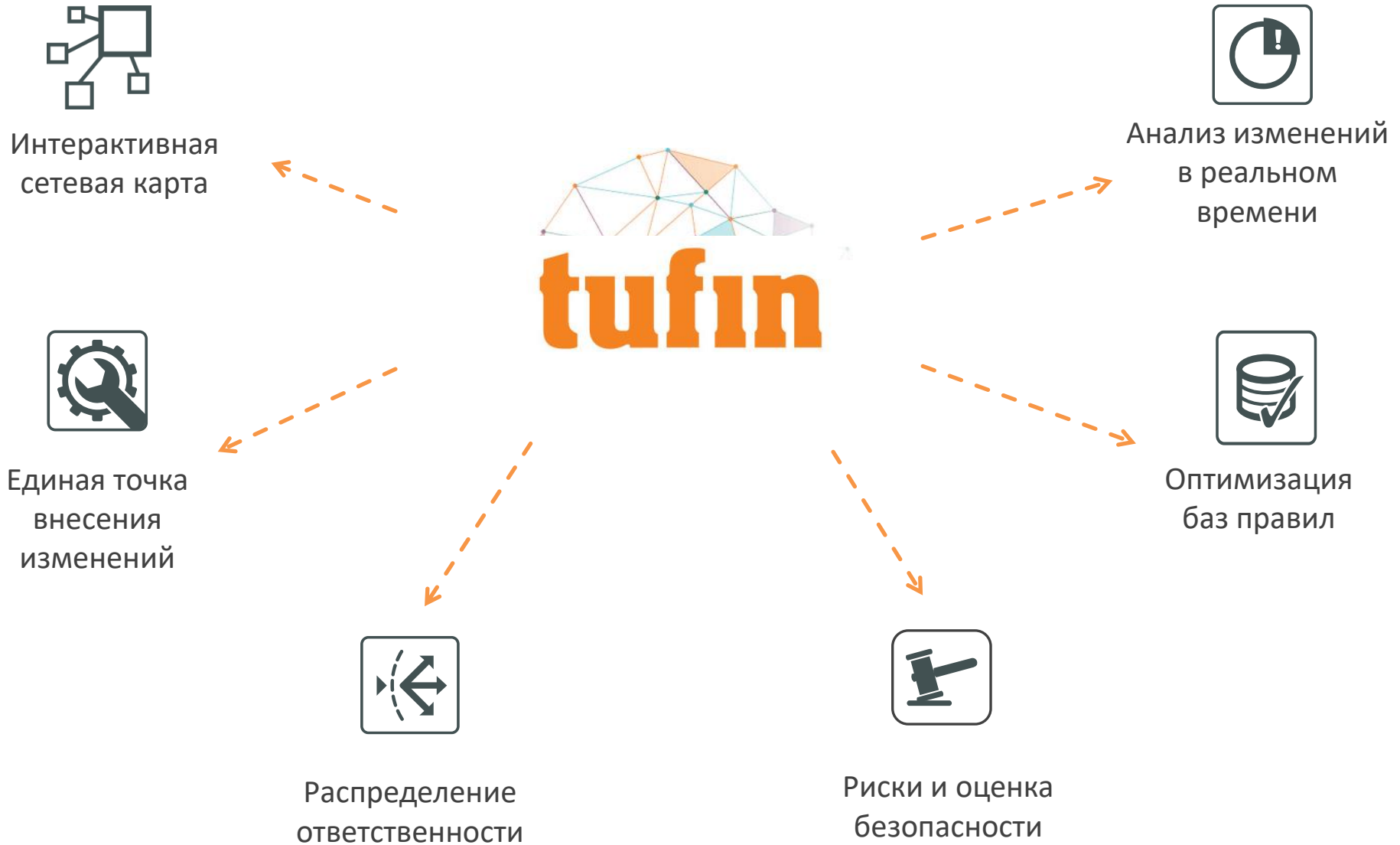


Ключевой пул поддерживаемых решений (примеры)

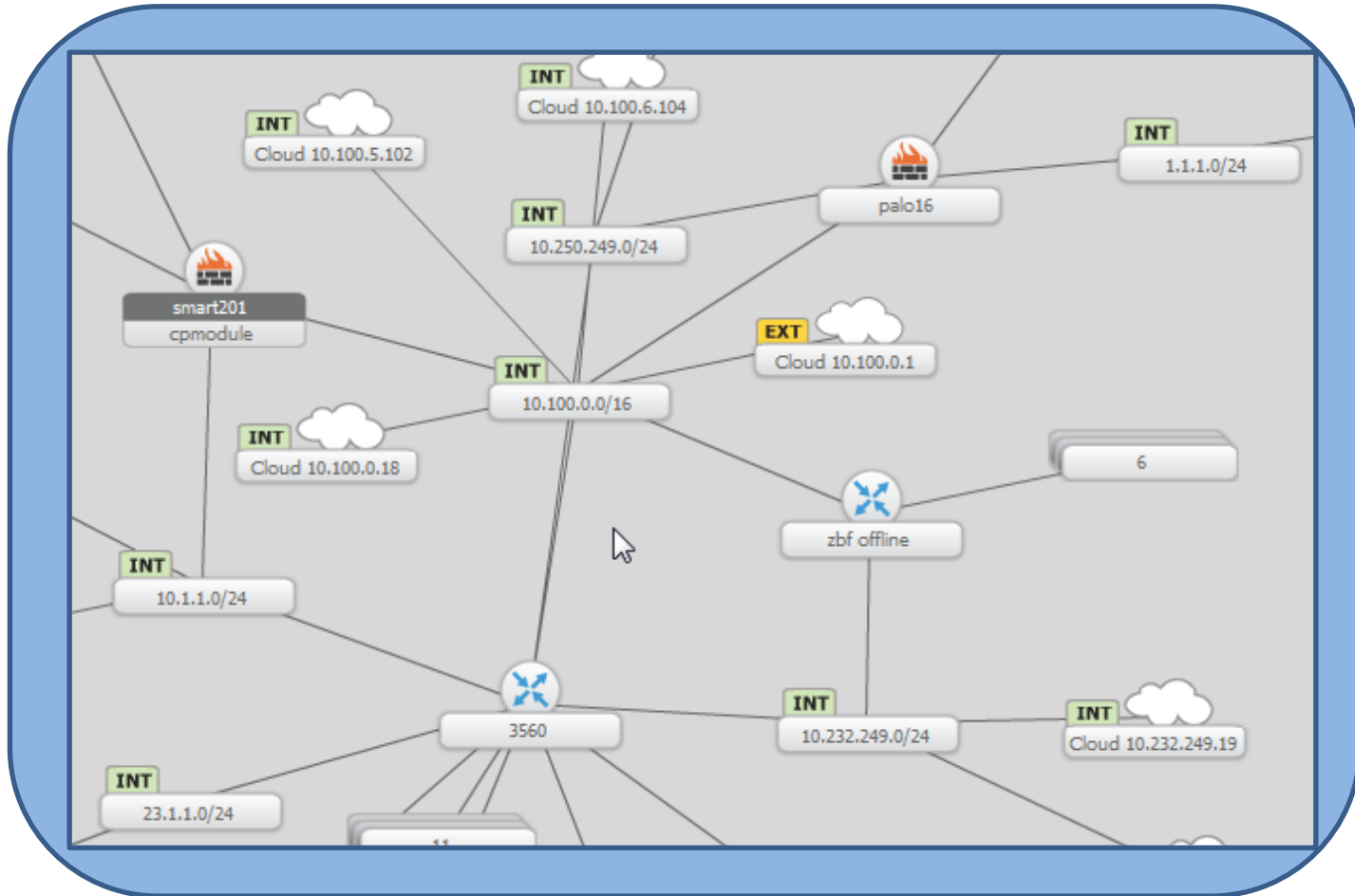


- ✓ Поддержка консолей управления и отдельных устройств от ведущих вендоров: Palo Alto (PA – Services/Users), Fortinet, Cisco, McAfee, Stonesoft, Forcepoint, Checkpoint, BlueCoat, Juniper, F5 BIG IP и другие...
- ✓ Все, что Linux на основе Red Hat - IPTables
- ✓ Коммутаторы, NLB, Generic Type

Ключевые блоки функционала Tufin TOS: работа с сетевым оборудованием



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



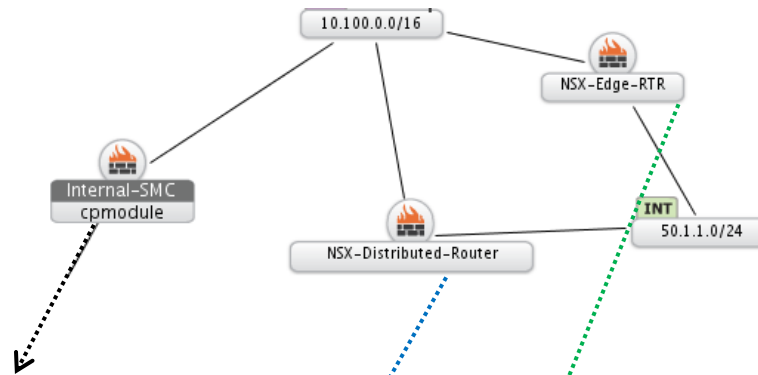
Хост



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	Default Rule	* Any	* Any	* Any
----	--------------------	--------------	-------	-------	-------

Анализ изменений в реальном времени (и история)

Rules | Objects | Running Config | Show IP Route | Interfaces | Routing | Zone Based Policy

Legend: Deleted (orange), Inserted (green), Modified (blue), Modified fields (yellow)

Access Rules | VPN Rules

Access List: 121
Inbound Interfaces: FastEthernet0/0

#	Action	Source Host/Network	Destination Host/Network	Service	Log Level	Description
1	✓	192.168.5.35	10.100.5.159	telnet/tcp		
2	✓	192.168.5.36	10.100.5.160	ssh/tcp		
3	✓	192.168.5.37	10.100.5.161	www/tcp		
4	✗	Any	Any	ip		

Были такие адреса

Access List: 121
Inbound Interfaces: FastEthernet0/0

#	Action	Source Host/Network	Destination Host/Network	Service	Log Level	Description
1	✓	192.168.5.35	10.100.5.159	telnet/tcp		
2	✓	192.168.5.35	10.100.5.159	ssh/tcp		
3	✓	192.168.5.35	10.100.5.159	www/tcp		
4	✓	Any	Any	ip		

Стало «разрешить» Сейчас такие адреса

Пару минут назад в правилах 2, 3 и 4

Сейчас в правилах 2, 3 и 4

Единая контролируемая точка внесения изменений

DSR These changes are recommended for your access request: Go to: Select

ISG-Bordeaux

CHECK POINT
CISCO
FORTINET
JUNIPER
ISG-Bordeaux
→ DMZ1 -> LAN1

```
ISG-Bordeaux
set address "DMZ1" "Host_10.100.5.62" 10.100.5.62 255.255.255.255
set address "LAN1" "Host_10.0.05.20" 10.0.5.20 255.255.255.255
set policy id 2 from "DMZ1" to "LAN1" "Host_10.100.5.62" "Host_10.0.05.20" "HTTPS" permit log
set address "Untrust" "Host_10.100.5.62" 10.100.5.62 255.255.255.255
set address "DMZ1" "Host_10.0.05.20" 10.0.5.20 255.255.255.255
set policy id 3 from "Untrust" to "DMZ1" "Host_10.100.5.62" "Host_10.0.05.20" "HTTPS" permit log
set policy id 4 from "Untrust" to "LAN1" "Host_10.100.5.62" "Host_10.0.05.20" "HTTPS" permit log
```

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

Единая контролируемая точка внесения изменений

The screenshot displays a configuration window for a rule named 'AR1' under the context 'External_access_out'. The rule is currently 'Inserted', as indicated by a green checkmark icon. The configuration table below shows the rule's parameters:

Action	Source Host/Network	Destination Host/Network	ACL	
✓	192.168.3.110	NetworkGroup_40	Datacenter_access_in	smtp/tcp

Additional interface elements include a 'Customize rule' link and a close button (X) in the top right corner of the configuration area.

- ✓ 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.

The screenshot displays the Tufin SecureTrack Cleanup interface for the Internal-SMC (90) configuration. The interface is divided into two main sections: a tree view on the left and a cleanup table on the right.

Tree View (Left): Shows a hierarchy of devices. The 'Internal-SMC' device is highlighted, indicating it is the selected configuration for cleanup.

Cleanup Table (Right): A table with columns 'Cleanup' and 'Name'. It lists four cleanup items:

Cleanup	Name
C01	Fully shadowed and redundant rules
C05	Disabled rules
C06	Unattached network objects
C11	Duplicate network objects

A red box highlights this table, and a red arrow points from the 'Internal-SMC' device in the tree view to it.

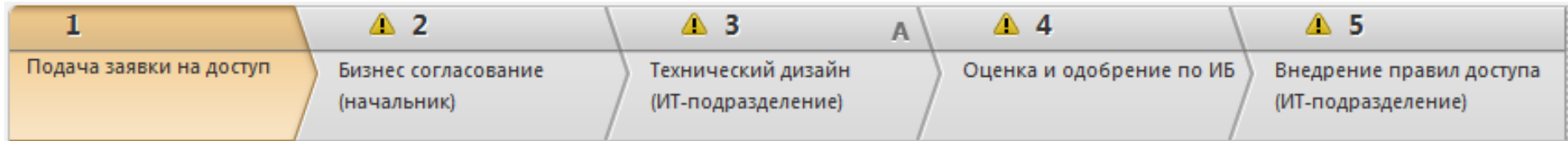
Standard Table (Bottom): A table with columns 'NO.', 'NAME', 'SOURCE', 'DESTINATION', 'VPN', and 'TCP/UDP'. It shows a single rule with ID 5:

NO.	NAME	SOURCE	DESTINATION	VPN	TCP/UDP
5		PCI_APP_2 PCI_APP_1	AD_SERVER	* Any	TCP/UDP

A red arrow points from the 'SOURCE' column of the cleanup table to the 'SOURCE' column of the Standard table.

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

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

Making Security Manageable

СПАСИБО ВАМ!