Целевое управление доступом в сети
Техническое решение для финансовых организаций

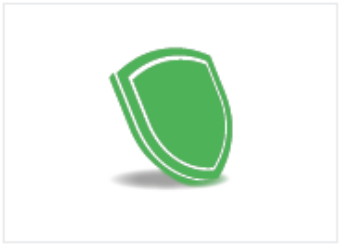
Александр Кушнарев,
Технический консультант,
Netwell Ltd.

О продукте, ключевые функции

1

Аналитическая часть: подключение к МЭ, коммутаторам, маршрутизаторам, WAN- оптимизаторам и т.п.

- Централизованная визуализация, оптимизация, оценка корректности и безопасности сетевого доступа в сети



SecureTrack

2

Процессы и автоматизация:

- Формализация процессов доступа на основе заявок
- Автоматизированное формирование и продвижение правил сетевого доступа

SecureChange

3

Работа с ключевыми приложениями организации:

- Защита доступа между компонентами, от и до приложений

SecureApp

tufin

Ключевые особенности и позиционирование

- ✓ Сетевые структуры и сегменты с оборудованием ведущих мировых производителей
- ✓ Сертификация: не является антивирусом, СОВ, МЭ. Думаем…
- ✓ Не требуется «писать коннекторы», все необходимое есть
- ✓ Рынок и спрос в России есть

tufin

В чем ценность решения для финансовых организаций?

1. Наведение и постоянное поддержание порядка в листах доступа (ACL) сетевого оборудования

2. Оценка безопасности и корректности правила сетевого доступа ДО его фактического применения

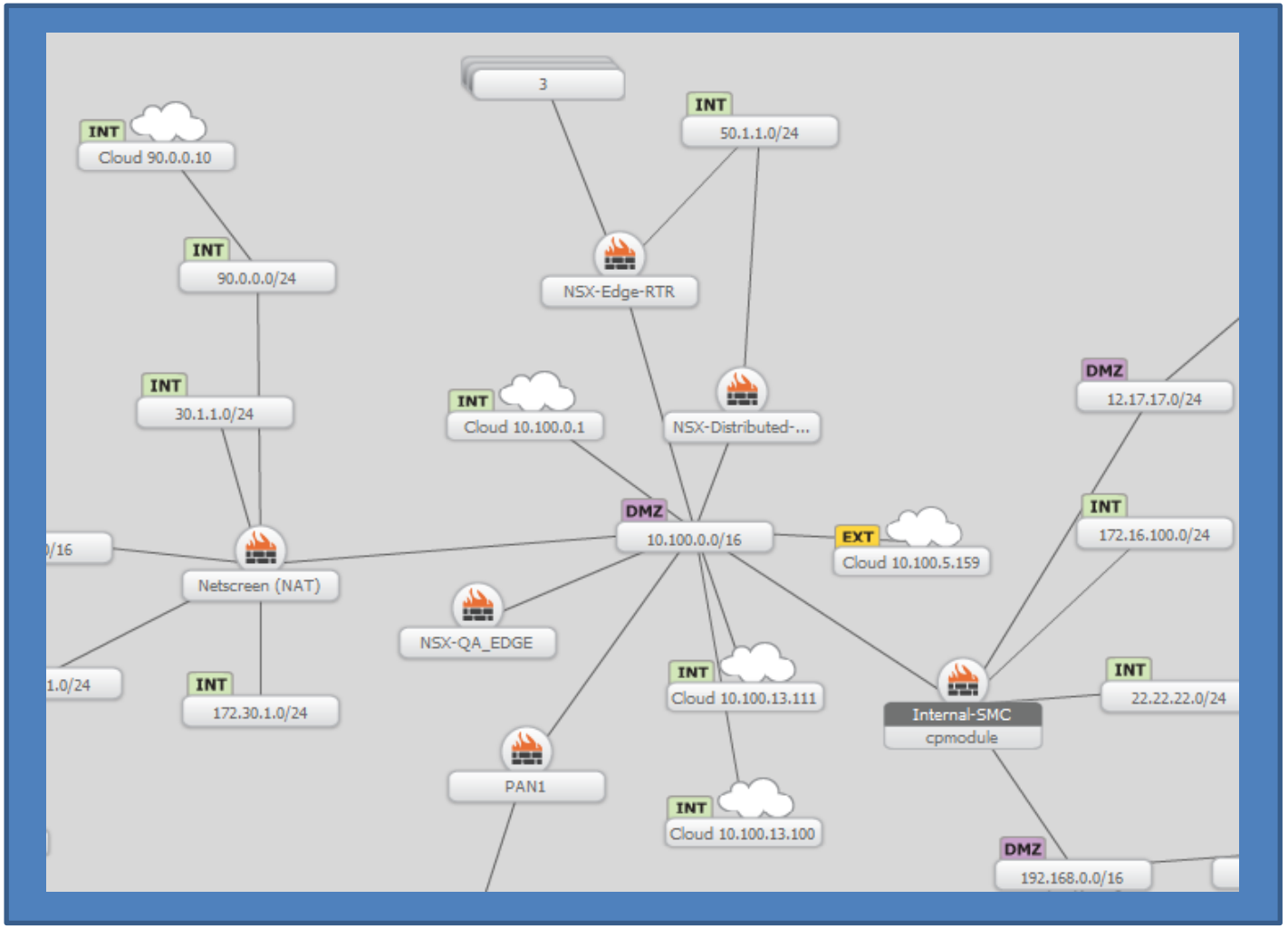
3. Автоматическое «продвижение» правил доступа в устройства разных производителей согласно тому, что уже есть

tufin

В чем ценность решения для финансовых организаций?

Каким образом это делаем с решением от Tufin?

Учитывает топологию, маршруты, интерфейсы, зоны, MPLS, NAT, VPN



tufin

В чем ценность решения для финансовых организаций?

Каким образом это делаем с решением от Tufin?

- Знаем архитектуру, синтаксис и строение ACL оборудования
- Понимаем уровень объектов (сервис, приложение, 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

В чем ценность решения для финансовых организаций?

Каким образом это делаем с решением от Tufin?

Распознаем риски по протоколам и приложениям

100 | Internal-SMC

Risk	Name	Type	Inst
N12	Telnet services can enter Internal and/or DMZ networks	Risky rules	2
N13	SNMP services can enter Internal and/or DMZ networks	Risky rules	1
E01	IRC services can exit Internal and/or DMZ networks	Risky rules	1
E02	Known P2P services can exit Internal and/or DMZ networks	Risky rules	1
E03	NNTP services can exit Internal and/or DMZ networks	Risky rules	1
E04	Any services can exit Internal and/or DMZ networks	Risky rules	1
I01	Risky Microsoft services are allowed from DMZ networks to Internal networks	Risky rules	1
I02	POP services are allowed from DMZ networks to Internal networks	Risky rules	1

Instances | Information

Show: Internal-SMC

Standard

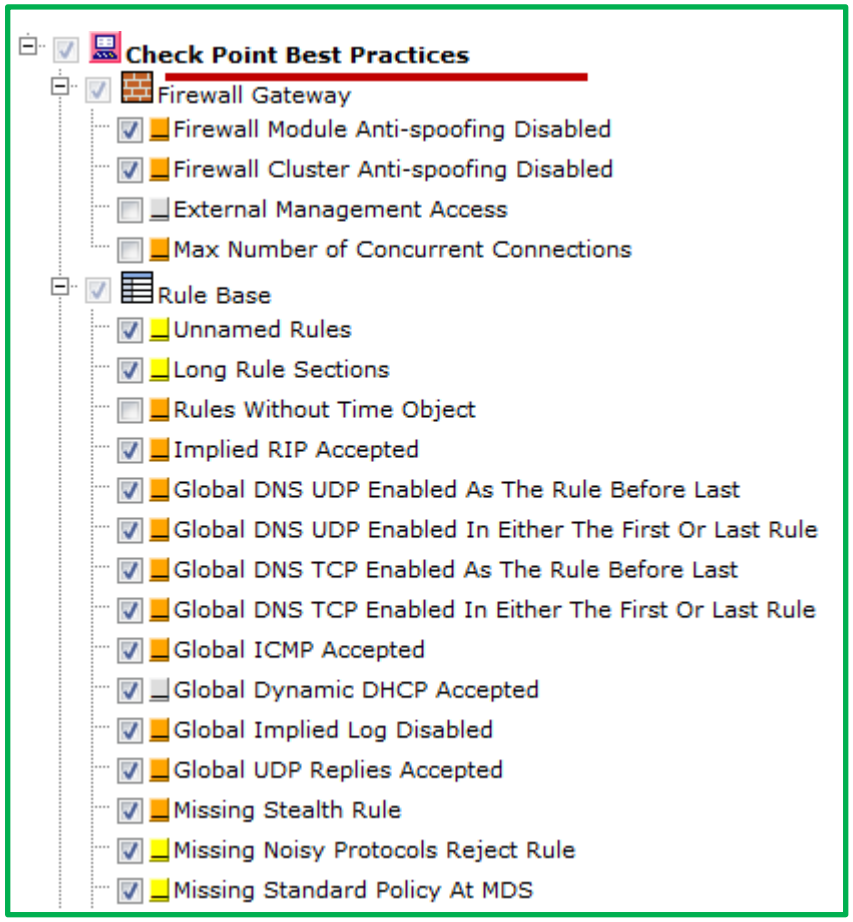
NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
3		Users_192.168.0.0	LAN	* Any	TCP HTTP_and_HTTPS...	Accept	Log	* Any	* Any	Users access to the web

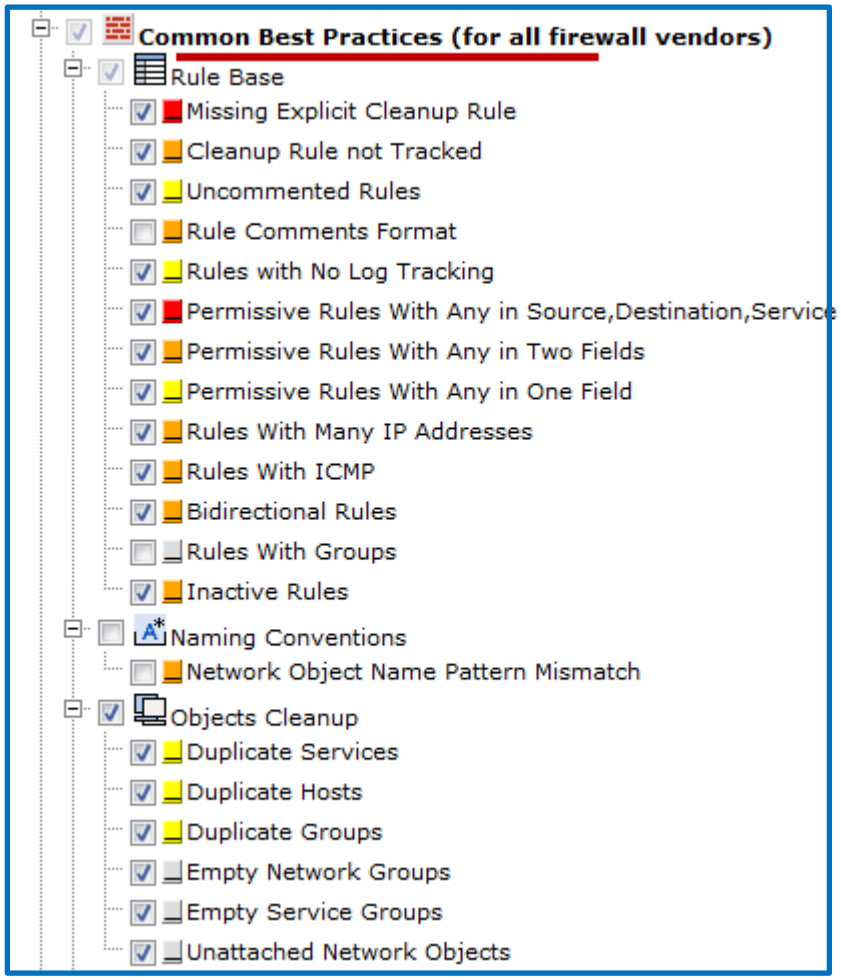
tufin

NETWELL

В чем ценность решения для финансовых организаций?

Каким образом это делаем с решением от Tufin?



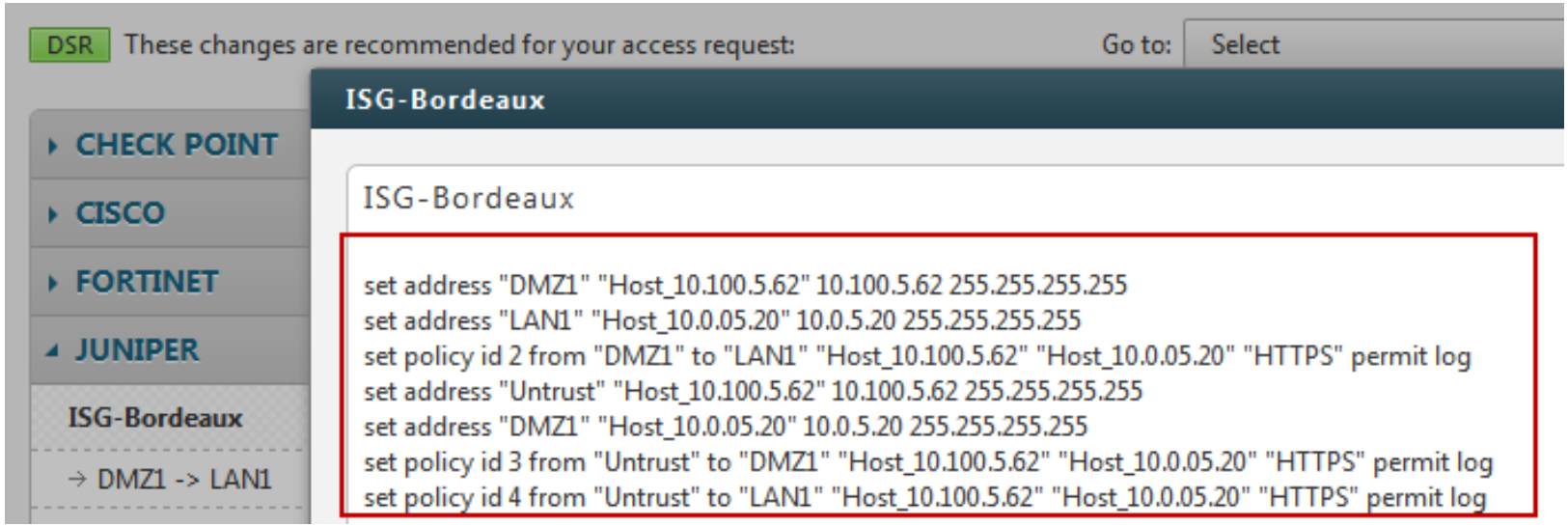


Оцениваем по базе наработанных годами практик конфигураций

В чем ценность решения для финансовых организаций?

Обладая вышеприведенной информацией:

- Система из простого запроса по заявке сформирует правило доступа
- Для **Cisco, Juniper, Checkpoint** – система может автоматически прописать правила

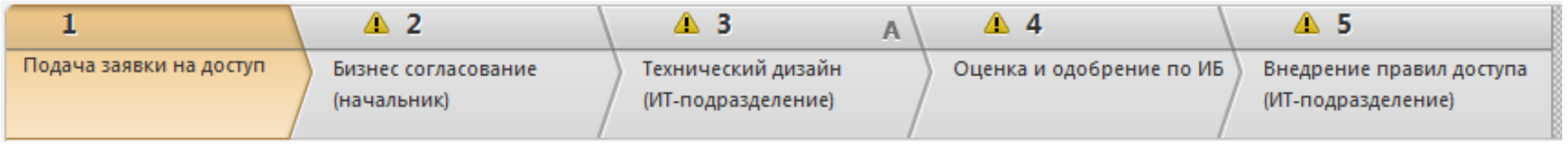


tufin

NETWELL

В чем ценность решения для финансовых организаций?

Формализация бизнес-процедур по доступу между IT и ИБ



Шаг 3: Технический дизайн (ИТ-подразделение):

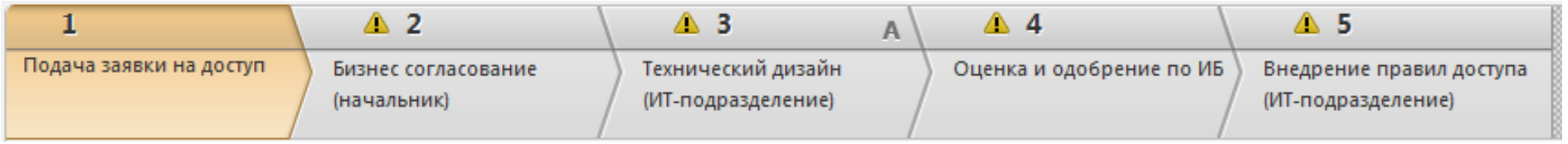
- Задаем откуда, куда и что
- Автопроверка «есть ли уже такой доступ» и где по цепочке?
- Дизайнер логического доступа: как изменить объекты, проверка по политикам ИБ, что изменить

Отвечаем только за то, за что необходимо

tufin

В чем ценность решения для финансовых организаций?

Формализация бизнес-процедур по доступу между IT и ИБ



Шаг 4: Оценка и одобрение по ИБ:

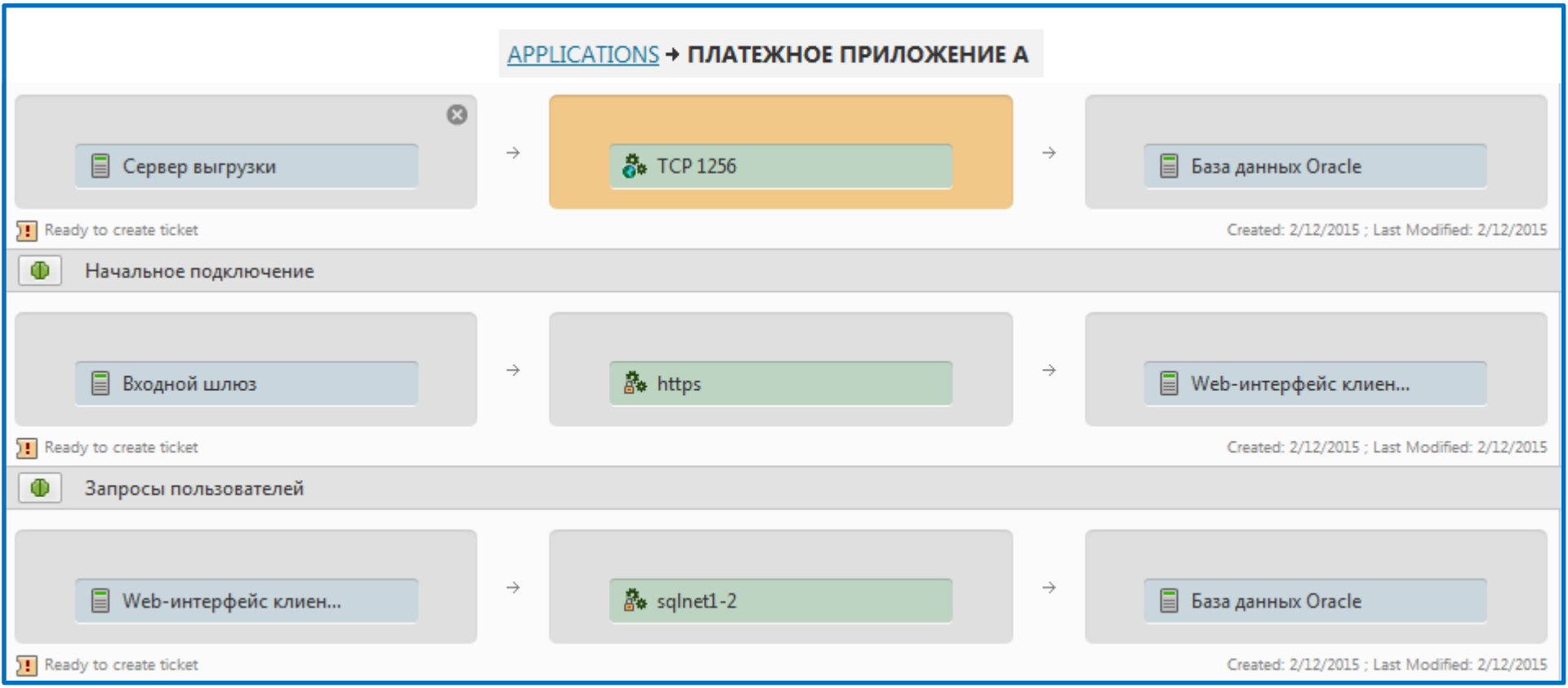
- Оценка в соответствии с базой рисков с учетом дизайна
- Выдача результатов проверки по политикам ИБ (для зон, серверов и т.п.) до внедрения
- Выдача утверждения, передача на этап внедрения

Отвечаем только за то, за что необходимо

tufin

В чем ценность решения для финансовых организаций?

Защита доступа к приложениям, между компонентами



- Определяем объекты (IP, приложения, протоколы, объекты из базы)
- Автоматически создается заявка с требуемыми правилами
- Устанавливаются правила и ведется наблюдение

СПАСИБО ВАМ!

Александр Кушнарев,
Технический консультант,
Netwell Ltd.
akushnarev@netwell.ru,

+7 (495) 66 239 66 доб. 1123