Ключевые задачи управления сетевым доступом

Александр Кушнарев,
Технический консультант,
Netwell Ltd.

Структура презентации

- ✓ Проблемы ЦУ доступом: когда актуально?
- ✓ Типовые потребности и задачи Заказчика
- ✓ Профиль клиентов в России
- ✓ Из чего состоит решение Tufin TOS?
- ✓ Ключевой функционал решения

Когда актуально?

- ✓ В сети компании – не менее пяти (5) сетевых устройств
- ✓ К таким устройствам относятся: коммутаторы, маршрутизаторы, межсетевые экраны (основное)
- ✓ Используется сетевое оборудование одного или нескольких производителей: Palo Alto, Fortinet, Juniper, Checkpoint, Cisco, F5 Networks, McAfee/Forcepoint/Stonesoft и др.
- ✓ Профиль деятельности не принципиален (стандартная TCP/IP сеть)

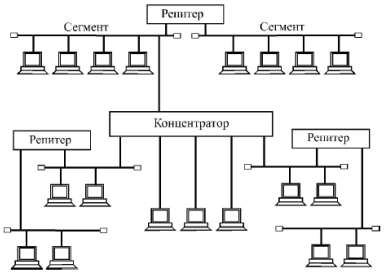
tufin

Что актуально? Типовые потребности и задачи Заказчика

- ✓ Анализ доступов любой сложности на оборудовании сети
  Оперативное выявление и устранение ошибок в инфраструктуре

- ✓ Оптимизация правил доступа на сетевом оборудовании:
  Фактическое снижение нагрузки на устройства до 30 – 50%

- ✓ Оценка рисков несанкционированного доступа в действующей структуре
  Устранение (изменение) опасных и потенциально опасных правил



Что актуально? Типовые потребности и задачи Заказчика

- ✓ Внесение в систему политик ИБ, контроль их исполнения
  Анализ изменений в доступе до его внесения в устройства

- ✓ Автоматическое написание и продвижение правил в сетевые устройства
  Один раз задаем условия – остальное система делает за нас

- ✓ Защита доступов ключевых бизнес-приложений
  Контроль доступности: платежных, биллинговых, финансовых и др. критически важных приложений

Из чего состоит решение Tufin TOS

SecureTrack

✓ Автоматизированный контроль и анализ сетевого доступа

Статистика, аналитика, соблюдение соответствия

Функционал, не предоставляемый консолями ЦУ отдельных производителей

SecureChange

✓ Система заявок и автоматическое продвижение изменений

Бизнес-процессы и автоматическое внесение изменений

Бизнес-процессы по доступу, автоматизация внедрения, оценка безопасности

SecureApp

✓ Управление доступностью приложений 24X7 в сети

Контроль и автоматизация доступов приложений

Модуль «охраны доступов» критически важных приложений

Профиль клиентов в России:

✓ **ФИНАНСОВЫЙ СЕКТОР**

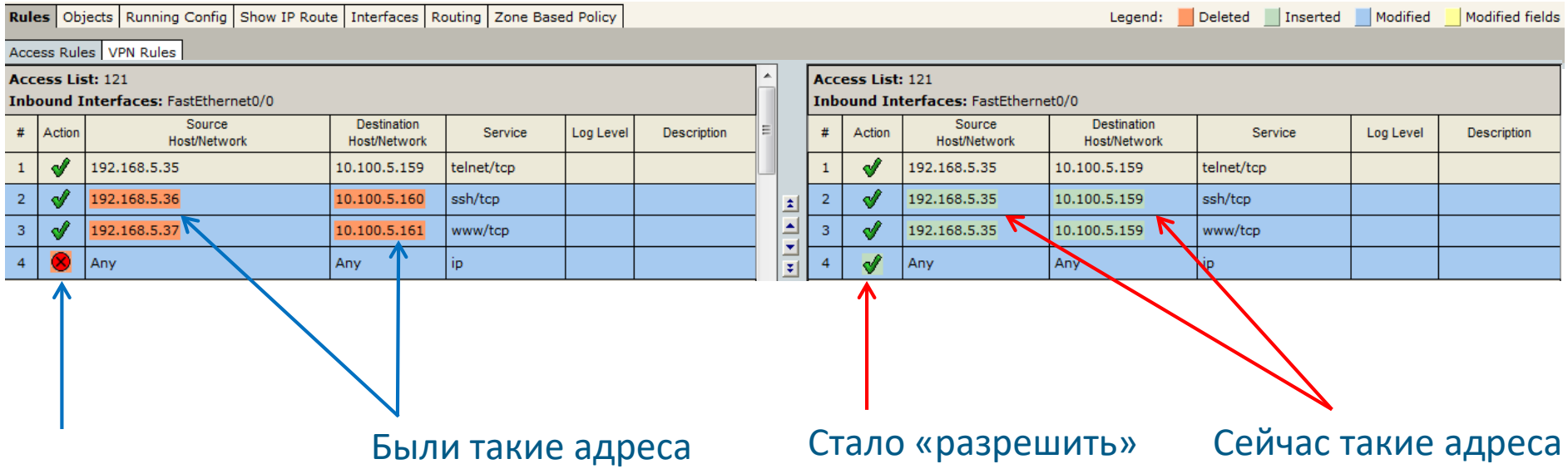
✓ **НЕФТЕГАЗОВЫЙ СЕКТОР**

✓ **ТЕЛЕКОММУНИКАЦИИ**

✓ **ПРОМЫШЛЕННОСТЬ И ДР.**

Внедрения в России есть – задачи Заказчиков понятны

Анализ изменений в реальном времени (и история)



Были такие адреса

Стало «разрешить»

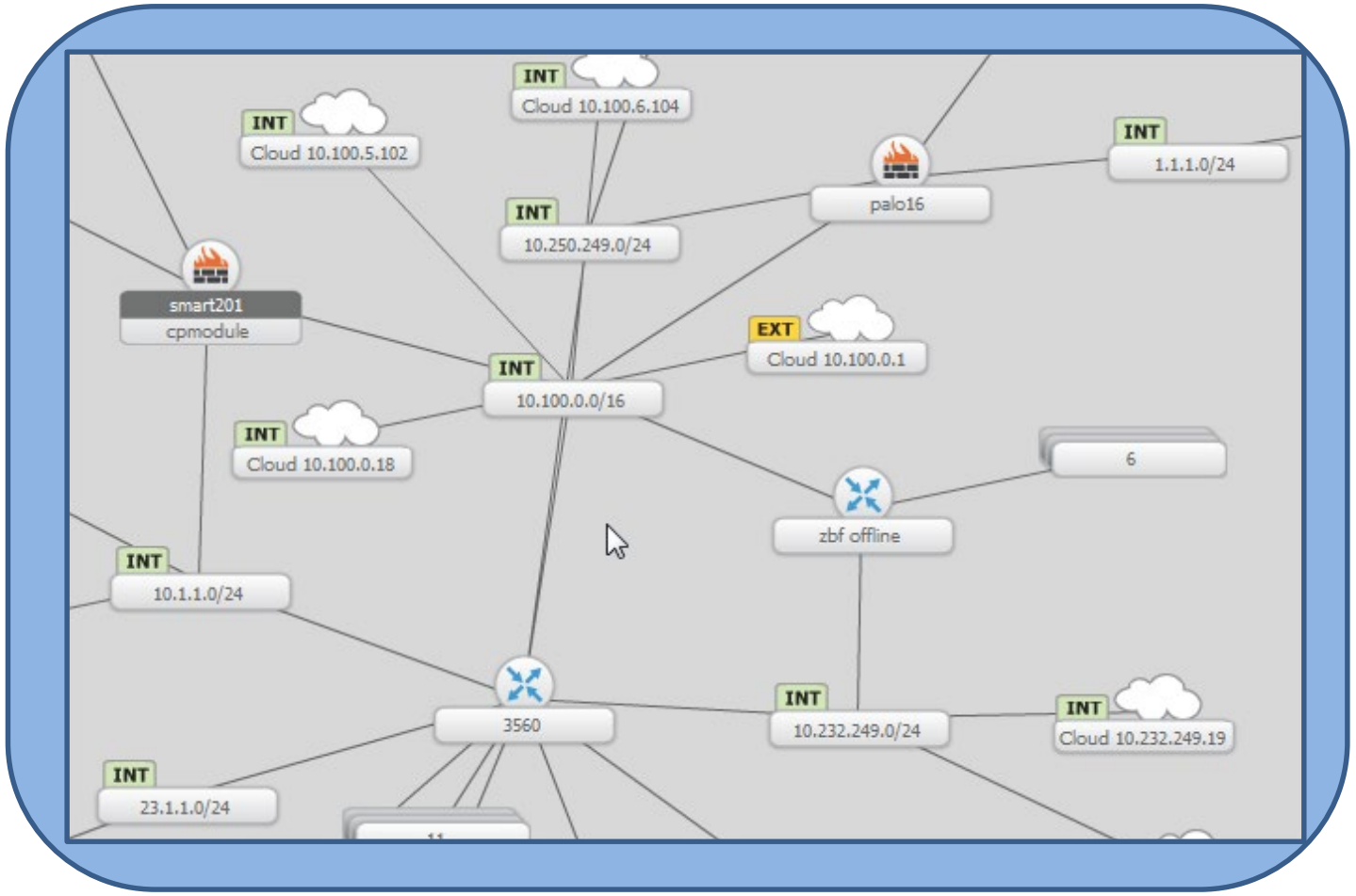
Сейчас такие адреса

Пару минут назад в правилах 2, 3 и 4

Сейчас в правилах 2, 3 и 4

tufin

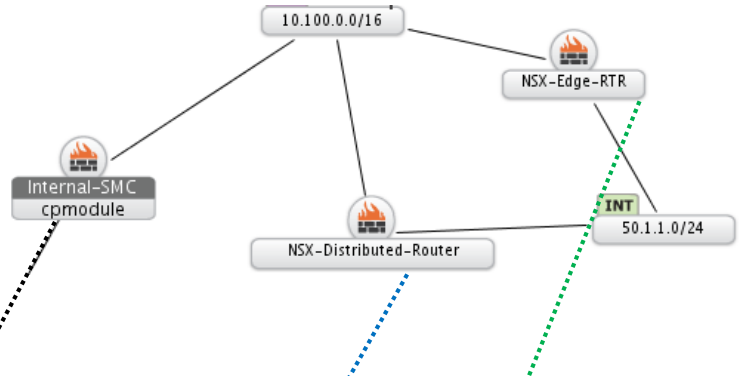
Сетевая топологическая карта



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

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

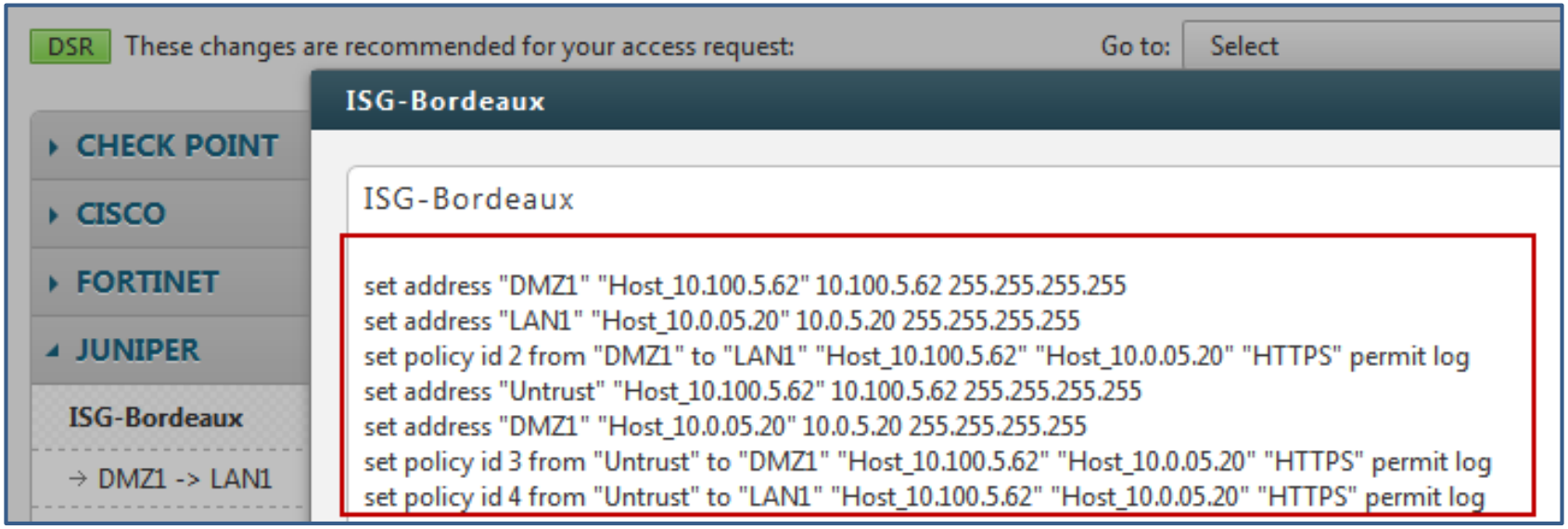
Сработает правило № 13, «пройдем»

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

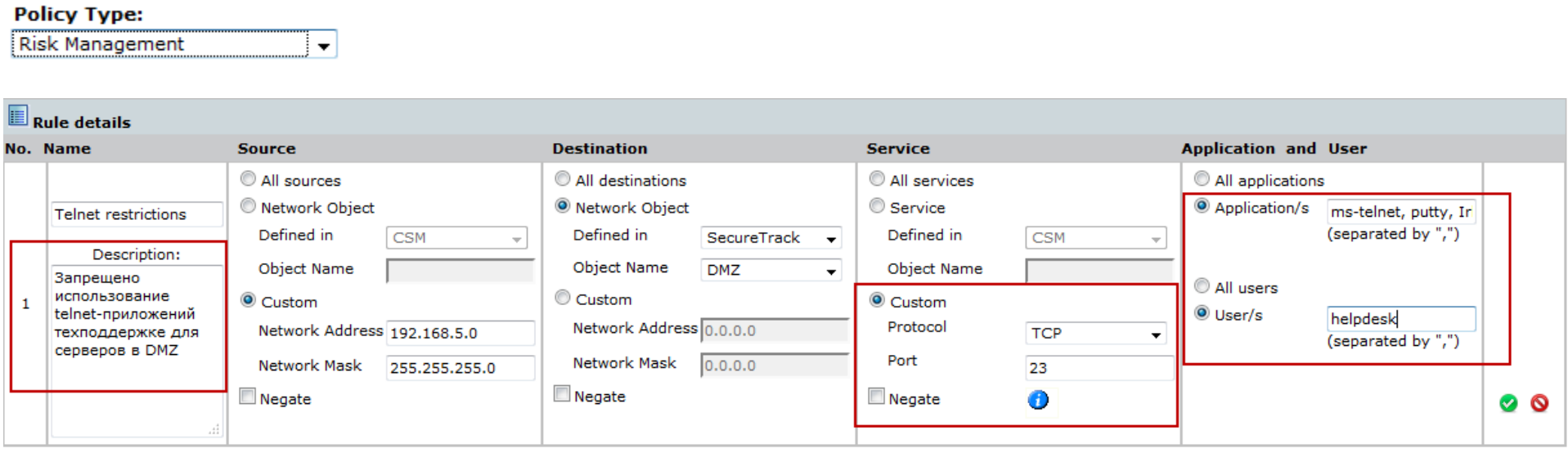
Единая контролируемая точка внесения изменений



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

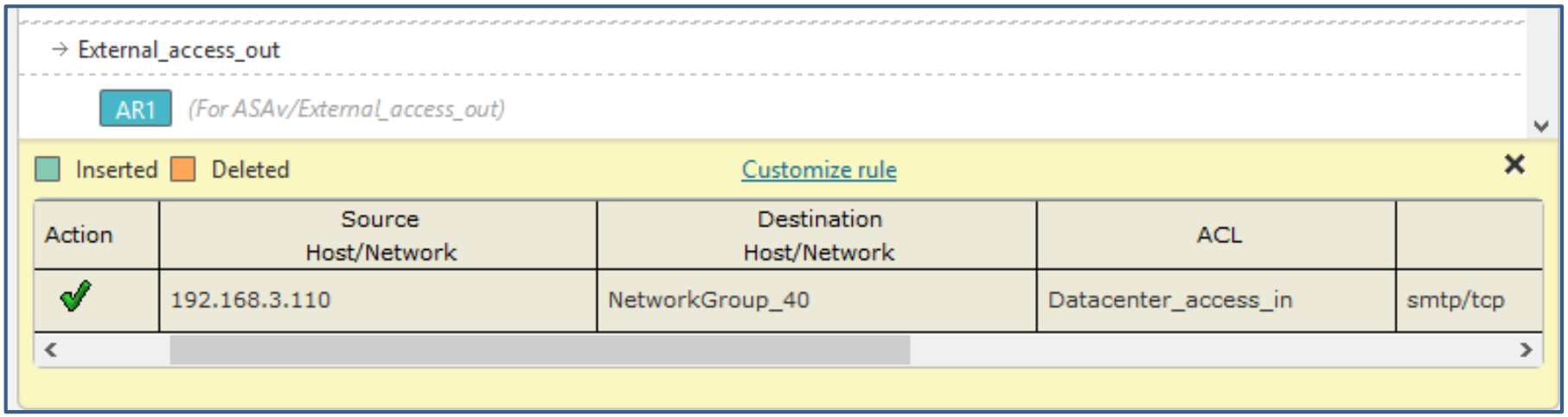
Проверка соответствия сетевого доступа политикам ИБ

Пример запрещающего условия



- ✓ Условие задается простыми понятиями: источник, назначение, порт-протокол, объект из базы устройства (для всего подключенного оборудования)
- ✓ Приложения и пользователи (для некоторых МЭ)

Единая контролируемая точка внесения изменений



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

СПАСИБО ВАМ!

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

+7 (495) 66 239 66