
# Tufin TOS: Целевой контроль логического доступа в сети

# **Tufin Software Technologies** - ключевой вендор Unified Firewalls Management

**2000**

клиентов по всему миру

**Сочетание:**

- **Аналитика**
- **Процессы**
- **Приложения**

- Израильская компания
- Основана в 2005 году

SC MAGAZINE BEST BUY ★★★★★

Info Security Products Guide 2013 GLOBAL EXCELLENCE BRONZE ★★★★★

2012 EMERGING vendors

NETWORK computing AWARDS 2012 FINALIST

SC MAGAZINE AWARDS 2012 EUROPE

Deloitte. Technology Fast50

# Реальные проблемы Заказчиков:

Есть политика защиты доступа по сети – но нет контроля управления изменениями. Почему?

1. Оборудование не меняют годами – правила доступа каскадные (100 >)
2. Там купили Palo Alto а там – Cisco, а тут подешевле еще есть Fortinet
3. Ни одна консоль ЦУ не покажет «А что если я так сделаю?»
4. Ни в одну консоль ЦУ не внесешь правила ИБ
5. «А кто в этом виноват?» - когда что-то случается (ИТ и ИБ)

# Ценность для IT-специалистов

## ✓ Средство организации и поддержки порядка в ACL:

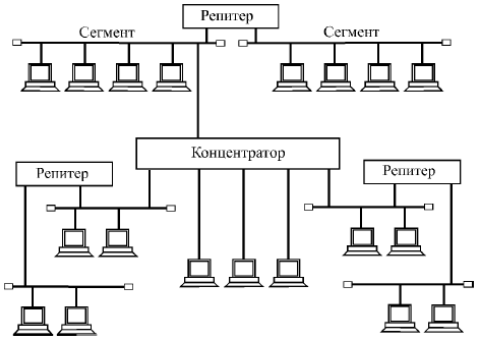
- Дублирующие, перекрывающие, неиспользуемые объекты и правила
- Фактическое использование правил – оптимизация

## ✓ Единая точка анализа и продвижения правил доступа:

- Единая консоль на Cisco, Checkpoint, Juniper, F5 и др.
- Контроль логического доступа в регионах
- Поддержка устаревшего оборудования и нестабильных каналов

## ✓ Оперативный анализ доступов любой сложности:

- Влияние NAT-правил, учета динамической и статической маршрутизации
- Поддержка виртуальных систем и ПАК (VMware + OpenStack)



# Для ИБ-специалистов

## ✓ Средство оценки приемлемости запрошенного доступа:

- Базы общих рисков («типовых ошибок»)
- Внесение в систему политик ИБ в виде простых правил МЭ

## ✓ Фиксация и формализация действий по доступу:

- Распределение ответственности по этапам обработки (шаблоны)
- Прямая привязка к техническому уровню, к сети

## ✓ Оперативная информация об изменениях в доступе:

- В реальном времени по факту изменения, по всей структуре;
- База событий за прошедшее время по всей структуре, PCI DSS 3.0


# Ключевой пул поддерживаемых решений


- Amazon
  - AWS EC2
- Check Point
  - CMA
  - SmartCenter
  - MDS
  - CLM/Log Server
- Cisco
  - PIX
  - ASA
  - FWSM
  - Router
  - XR Router
  - Nexus
  - Switch
  - L3 Switch
  - CSM
- Juniper
  - NetScreen
  - SRX, J-series
  - M,MX
  - NSM
- OpenStack
  - Cloud
- Fortinet
  - Fortigate
  - FortiManager
- Palo Alto Networks
  - PanOS
  - Panorama
- McAfee
  - Firewall Enterprise
- VMware
  - NSX
- F5
  - BIG IP
- Stonesoft
  - Management Center
- BlueCoat (TOP plugin)
  - AV
  - ProxySG
- Cisco-TOP (TOP plugin)
  - Catalyst
  - Ironport ESA
  - CSS
- Juniper-TOP (TOP plugin)
  - SA
- Linux (TOP plugin)
  - iptables

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

# Из чего состоит решение Tufin TOS

SecureTrack

- ✓ Автоматизированный контроль и анализ сетевого доступа
- ✓ На уровне сетевого оборудования от разных вендоров
- ✓ IT- подразделения, сетевые специалисты, сисадмины

Функционал, не предоставляемый консолями ЦУ отдельных производителей

SecureChange

- ✓ Формирование и обработка заявок доступа в сети
- ✓ Анализ корректности дизайна, рисков и безопасности
- ✓ ИБ-подразделения, не технические сотрудники

Бизнес-процессы по доступу, автоматизация внедрения, оценка безопасности

SecureApp

- ✓ Контроль доступности приложений 24X7 в сети
- ✓ Блокировка нарушений связи между и к приложениям
- ✓ Отделы разработки, обслуживание платежных систем

Модуль «охраны доступов» критически важных приложений

# Функционал SecureTrack

**Централизованный контроль логического доступа по всей сети:**

- На межсетевых экранах, коммутаторах, маршрутизаторах и другом сетевом оборудовании

**Проверка соответствия сетевого доступа политикам ИБ:**

- Блок общих рисков (ошибки конфигурации)
- Блок частных рисков (задаем собственные условия)

**Анализ политик доступа на используемость и безопасность:**

- Нахождение неиспользуемых правил и объектов внутри них, оптимизация используемых правил по трафику
- Рекомендации по сужению области действия правил (APG)

# Функционал SecureTrack

## Централизованный контроль логического доступа по всей сети

### Каким образом это делаем с решением от Tufin?

- Централизовано отображаем ACL («листы доступа») сетевого оборудования разных производителей

- Используем подключение по SSH или защищенным технологиям самих производителей оборудования

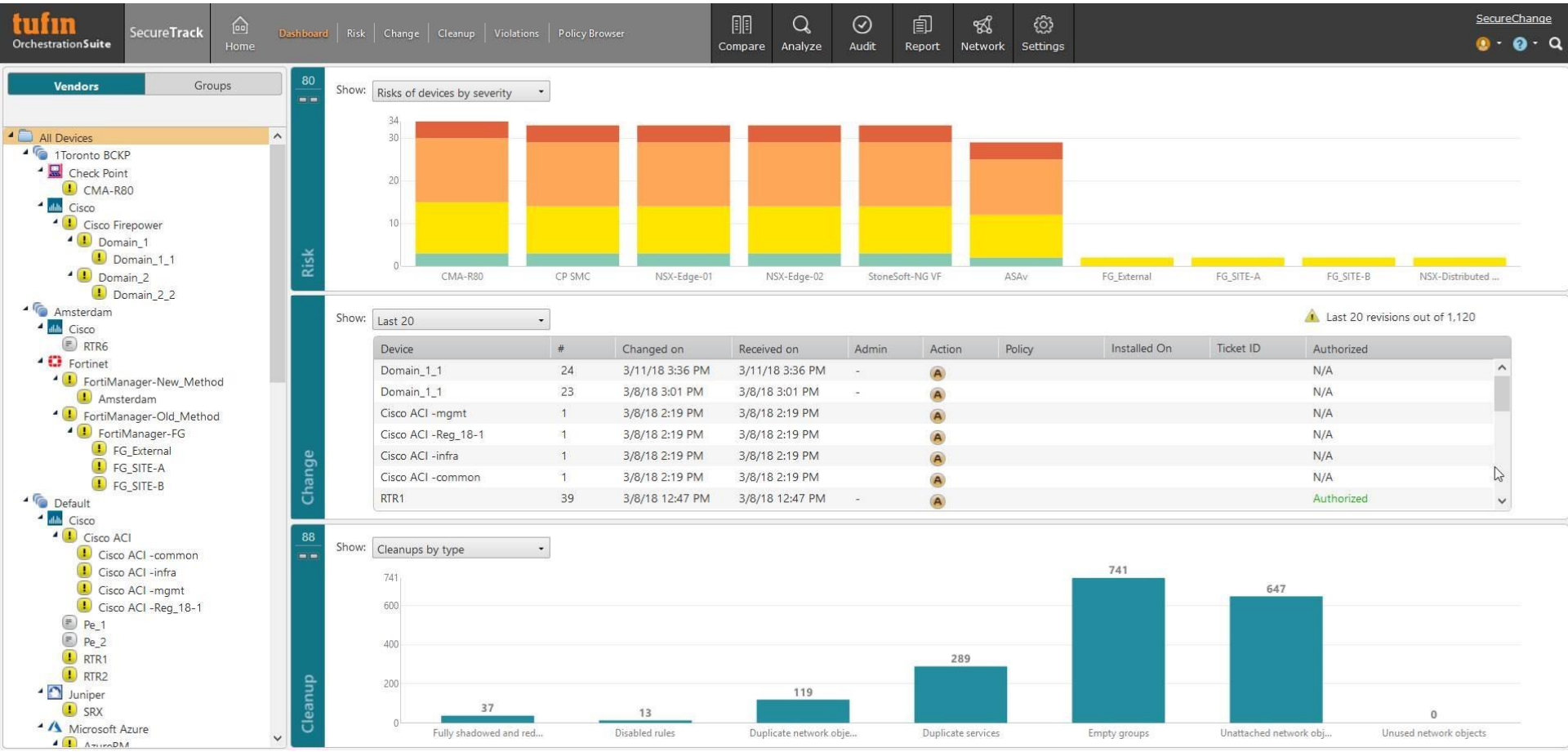
- Получаем оповещение о внесенном изменении (онлайн и/или по опросу)

- Видим контекст изменения: какая учетная запись, что изменилось, когда, откуда

# Функционал SecureTrack

## Централизованный контроль логического доступа по всей сети

Все устройства, а также последние изменения на них отображаются на Dashboard

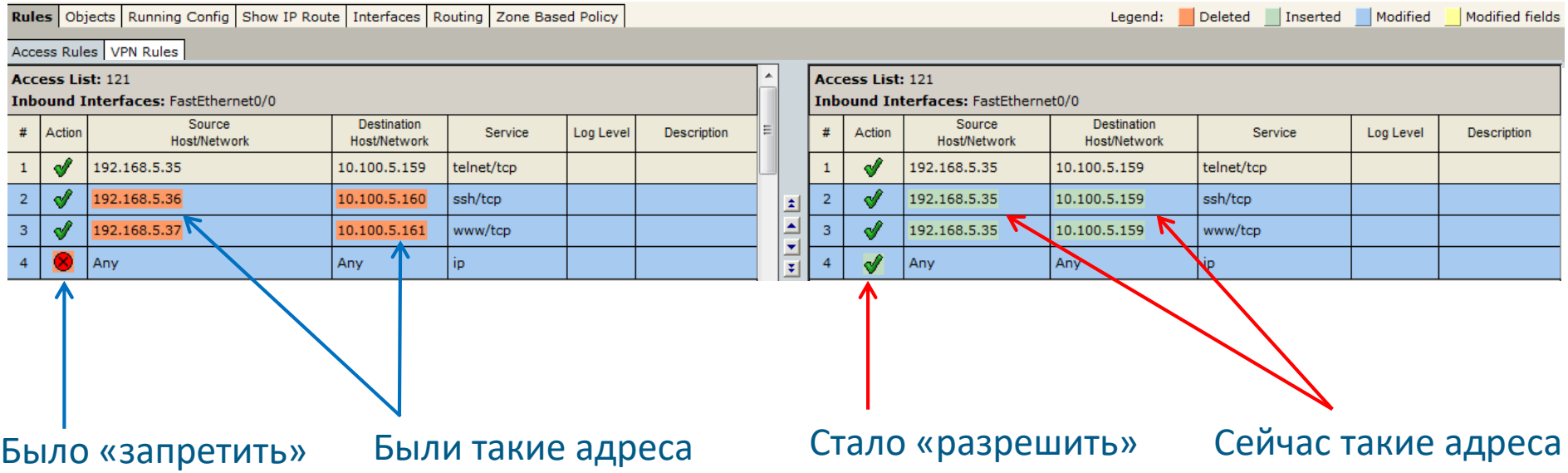


# Функционал SecureTrack

## Централизованный контроль логического доступа по всей сети

## Каким образом это делаем с решением от Tufin?

## Пример: межсетевой экран (удаленный или локальный)




Было «запретить»

Были такие адреса

Стало «разрешить»

Сейчас такие адреса

**Пару минут назад в правилах 2, 3 и 4**

**Сейчас в правилах 2, 3 и 4**

# Функционал SecureTrack

## Централизованный контроль логического доступа по всей сети

### Кто изменил доступ, когда и откуда?

**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 | | |

**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 | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 164 | | 23/11/14 14:57 | admin | cpmodule | EldadG-Laptop | 276760 | Standard_Prod - |

Дата/время изменения

Учетная запись на МЭ

Компьютер пользователя (для некоторых МЭ)

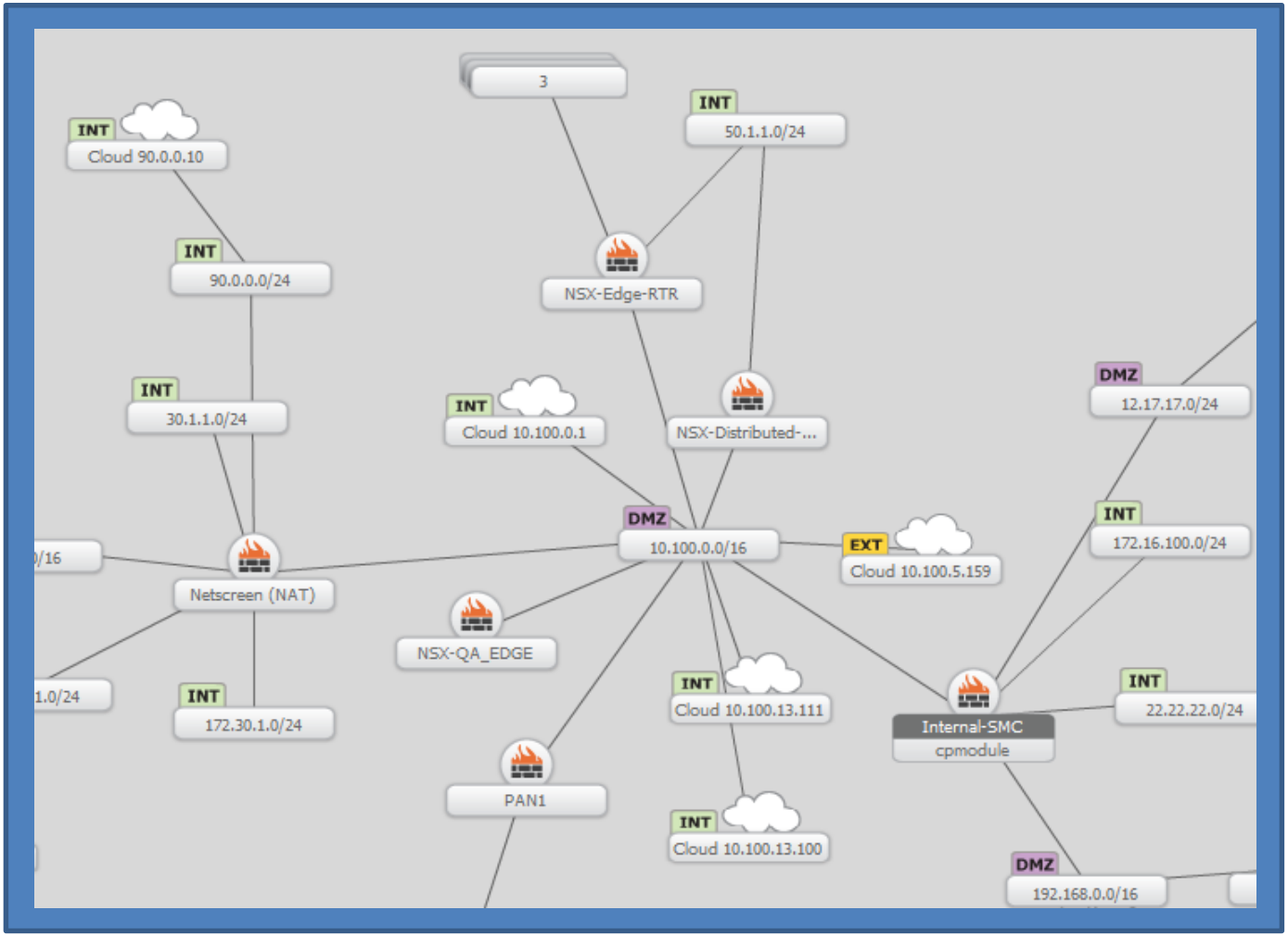
Набор политик

# Функционал SecureTrack

## Централизованный контроль логического доступа по всей сети

### Каким образом это делаем с решением от Tufin?

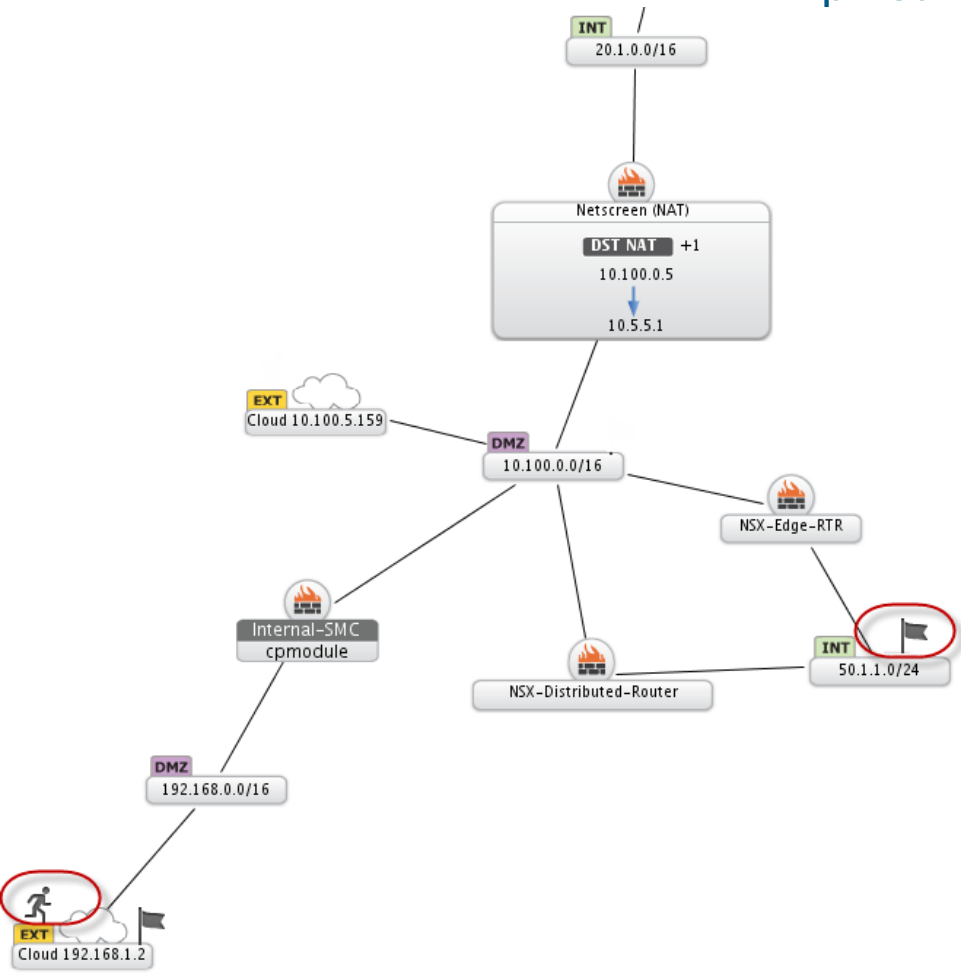
**Учитываем топологию, маршруты, интерфейсы, зоны, MPLS, NAT, VPN**



# Функционал SecureTrack

## Централизованный контроль логического доступа по всей сети

При запросе в интерфейсе системы Tufin TOS:




- Какой фактический сетевой доступ есть из «точки А» в точку «точку М»?

- Задаем интересующие сервисы, адреса, приложения и объекты из базы оборудования защиты

Сервис

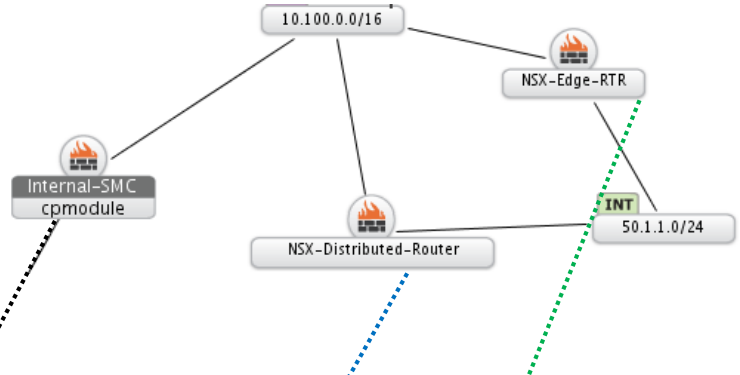

Хост

Приложение

# Функционал SecureTrack

## Централизованный 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<br>ipset_range<br>test_icon<br>MGMT-PortGroup | | DC_test2<br>MGMT<br>MGMT-PortGroup<br>none | | Data Recovery Appliance<br>DNS<br>UDP_500 |

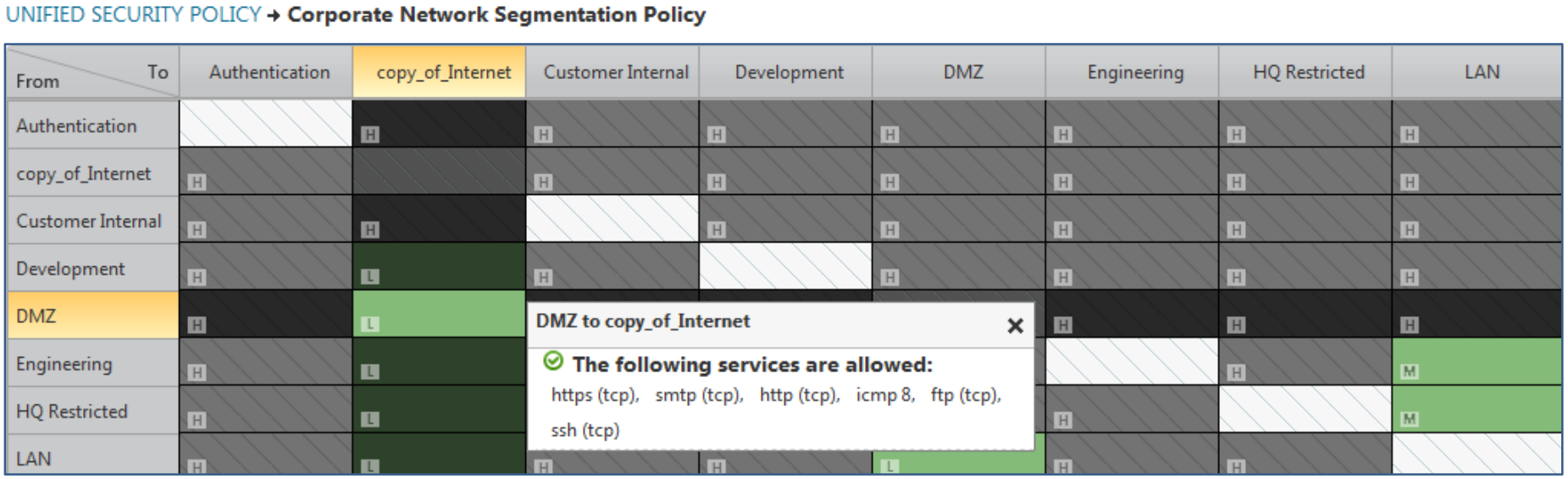
Такого доступа не будет, сработает правило № 53

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

# Функционал SecureTrack

## Матрица доступа для логических сегментов сети

- Определяем в Tufin зоны (логические сегменты)
- Устанавливаем между ними разрешенные или запрещенные доступы
- Система автоматически «накладывает» требования на сетевую карту, к нужным устройствам
- В каждом сетевом устройстве видим, какие правила и чему не соответствуют
- Инструмент приведения «того, что есть» к тому «как должно быть»



# Функционал SecureTrack

## Проверка соответствия сетевого доступа политикам ИБ

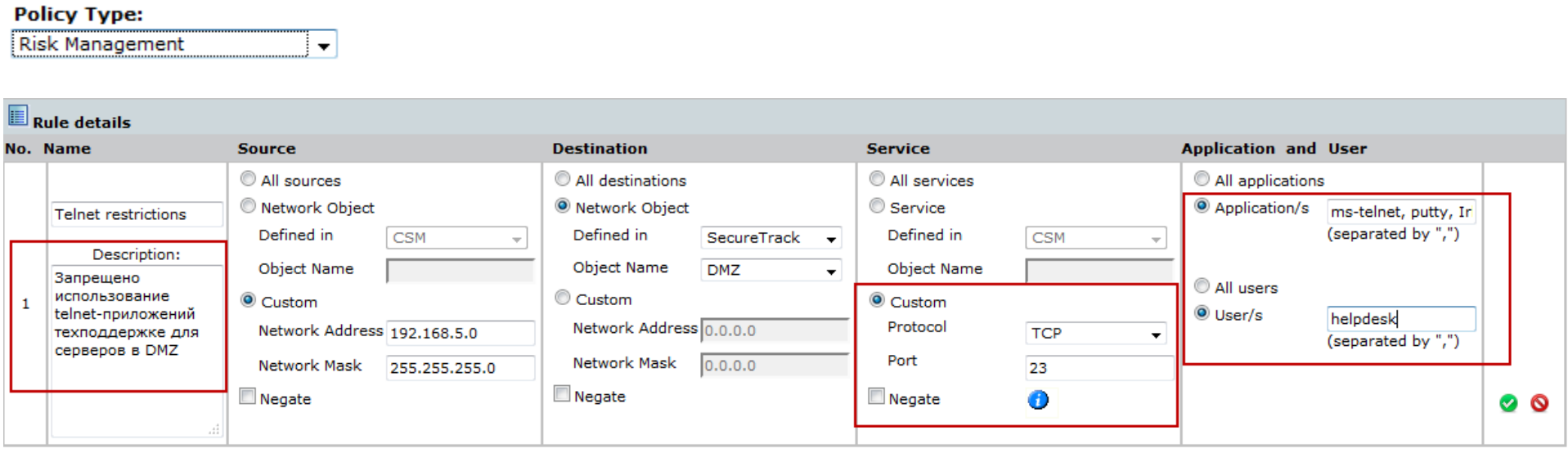
### Каким образом это делаем с решением от Tufin?

- Задаем политики доступа по сети к целевым системам разных видов в виде простых условий (оперируем IP-адресами, зонами, сегментами, сервисами)
- Первый вид условий: какого доступа никогда не должно быть, какие бы изменения не происходили
- Второй вид условий: какой доступ всегда должен быть, какие бы изменения не происходили

# Функционал SecureTrack

## Проверка соответствия сетевого доступа политикам ИБ

### Блок частных рисков - 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)

# Функционал SecureTrack

## Проверка соответствия сетевого доступа политикам ИБ

### Дополнительно к частным – есть «блок общих рисков»

**100** | Internal-SMC

| Risk | Name | Type | Ins |
|---|---|---|---|
| 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 |

- ✓ В блоке – правила проверки наличия доступа между DMZ, внутренними и внешними сетями по «рисковым» сервисам.
- ✓ То есть сервисов, для которых могут активно применяться эксплойты.
- ✓ Отображение соответствующих правил из базы сетевых устройств (онлайн).

# Функционал SecureTrack

## Проверка соответствия сетевого доступа политикам ИБ

### Что получаем в одном отчете?

Нарушение частных условий

Нарушение «общих» рисков

Уровень критичности

**Ссылка на нарушающие правила**

**Risks summary:**

| # | Code | Risk | Severity | Status | Details |
|---|---|---|---|---|---|
| 1 | C009 | Compliance policy "Allowed business traffic" | Critical | Failed | 1 violations |
| 2 | C002 | Compliance policy "Business Critical Access" | Critical | Failed | 3 violations |
| 3 | C011 | Compliance policy "Compliance Policy 12/11/2013" | Critical | Failed | Details |
| 4 | C010 | Compliance policy "Telnet restriction" | Critical | Failed | 5 violations |
| 5 | S004 | Any service is allowed from the DMZ network(s) to the Internal network(s) | Critical | Failed | 1 violations |
| 6 | I004 | HTTP/HTTPS services from DMZ to internal | Critical | Failed | 4 violations |
| 7 | I003 | IMAP services from DMZ to internal | Critical | Failed | 1 violations |
| 8 | I002 | POP services from DMZ to internal | Critical | Failed | 1 violations |
| 9 | I001 | Risky Microsoft services from DMZ to internal | Critical | Failed | 1 violations |
| 10 | S016 | More than 1000 UDP from DMZ to internal | High | Failed | 1 violations |
| 11 | S015 | More than 1000 TCP from DMZ to internal | High | Failed | 1 violations |
| 12 | S013 | More than 1000 UDP services can leave the network(s) | High | Failed | 1 violations |
| 13 | S012 | More than 1000 TCP services can leave the network(s) | High | Failed | 1 violations |
| 14 | S007 | Any service can leave the network(s) | High | Failed | 1 violations |
| 15 | E001 | IRC services can leave the network | High | Failed | 1 violations |
| 16 | N013 | SNMP services can enter the network | Medium | Failed | 1 violations |
| 17 | N012 | Telnet services can enter the network | Medium | Failed | 2 violations |
| 18 | E002 | Known P2P services can leave the network | Medium | Failed | 1 violations |
| 19 | E003 | NNTP services can leave the network | Low | Failed | 1 violations |

- ✓ Запускаем отчет по запросу или по расписанию (выбранные устройства или все)
- ✓ Видим нарушения политик ИБ по доступу и рекомендациям «общих рисков».
- ✓ Для каждого нарушения – интерактивная ссылка на соответствующие правила.

# Функционал SecureTrack

## Оптимизация правил и политик доступа (оптимизация ACL)

- Неиспользуемые правила и объекты внутри них
- Фактическое использование правил – оптимизация по трафику
- Рекомендация по сужению области действия правил (APG) и многое другое

| NO. | HITS | FIRST HIT | LAST HIT | NAME | SOURCE | DESTINATION | VPN | SERVICE | ACTION | TRA |
|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 1,161,898 (73%) | Thu, 09 Oct 2014 07:00 | Mon, 08 Dec 2014 04:00 | | Users_192.168.0.0 1,161,898 (100%) | LAN | * Any | * Any | accept | Lo |
| 2 | 264,009 (17%) | Thu, 09 Oct 2014 07:00 | Mon, 08 Dec 2014 04:00 | | LAN_192.168.0.0 264,009 (100%) | LAN_192.168.0.0 264,009 (100%) | * Any | * Any | accept | Lo |

**Least-used rules - 2 of 40 (bottom 50%)**

| NO. | HITS | FIRST HIT | LAST HIT | NAME | SOURCE | DESTINATION | VPN | SERVICE | ACTI |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 156,630 (10%) | Thu, 09 Oct 2014 10:00 | Sat, 06 Dec 2014 06:00 | Comment | Mgmt_Net_192.168.5.0 0 (0%)<br>Mgmt_Net_192.168.3.0 0 (0%)<br>st_192.168.3.30 0 (0%)<br>DemoTSS 0 (0%)<br>qa_10.100.6.210 0 (0%)<br>Mgmt_Net_192.168.4.0 0 (0%)<br>CP_default_Office_Mode_addresses_pool 156,630 (100%)<br>QA_10.100 0 (0%) | cpmodule 156,630 (100%) | * Any | TCP CPMI 0 (0%)<br>TCP FW1_ica_pull 0 (0%)<br>TCP ssh 0 (0%)<br>UDP snmp 0 (0%)<br>TCP FW1_lea 156,630 (100%) | acce |
| 2 | 264,009 (17%) | Thu, 09 Oct 2014 07:00 | Mon, 08 Dec 2014 04:00 | | LAN_192.168.0.0 264,009 (100%) | LAN_192.168.0.0 264,009 (100%) | * Any | * Any | acce |

# Функционал SecureTrack

## Оптимизация правил и политик доступа (оптимизация ACL)

- Tufin анализирует правило на протяжении заданного периода времени и выдаёт рекомендация по сужению области его действия

tufin OrchestrationSuite | SecureTrack | Home | Compare | Analyze | Policy Analysis | Object Lookup | Automatic Policy Generator | Audit | Report | Network | Settings

Back to job list

APG results for: FMG-APG-01

Save rule set | Replacement rules for export | Balance graph

Permissiveness of original selected rule: **23**
Highest permissiveness for automatically generated rules: **32**
Number of rules: **7**

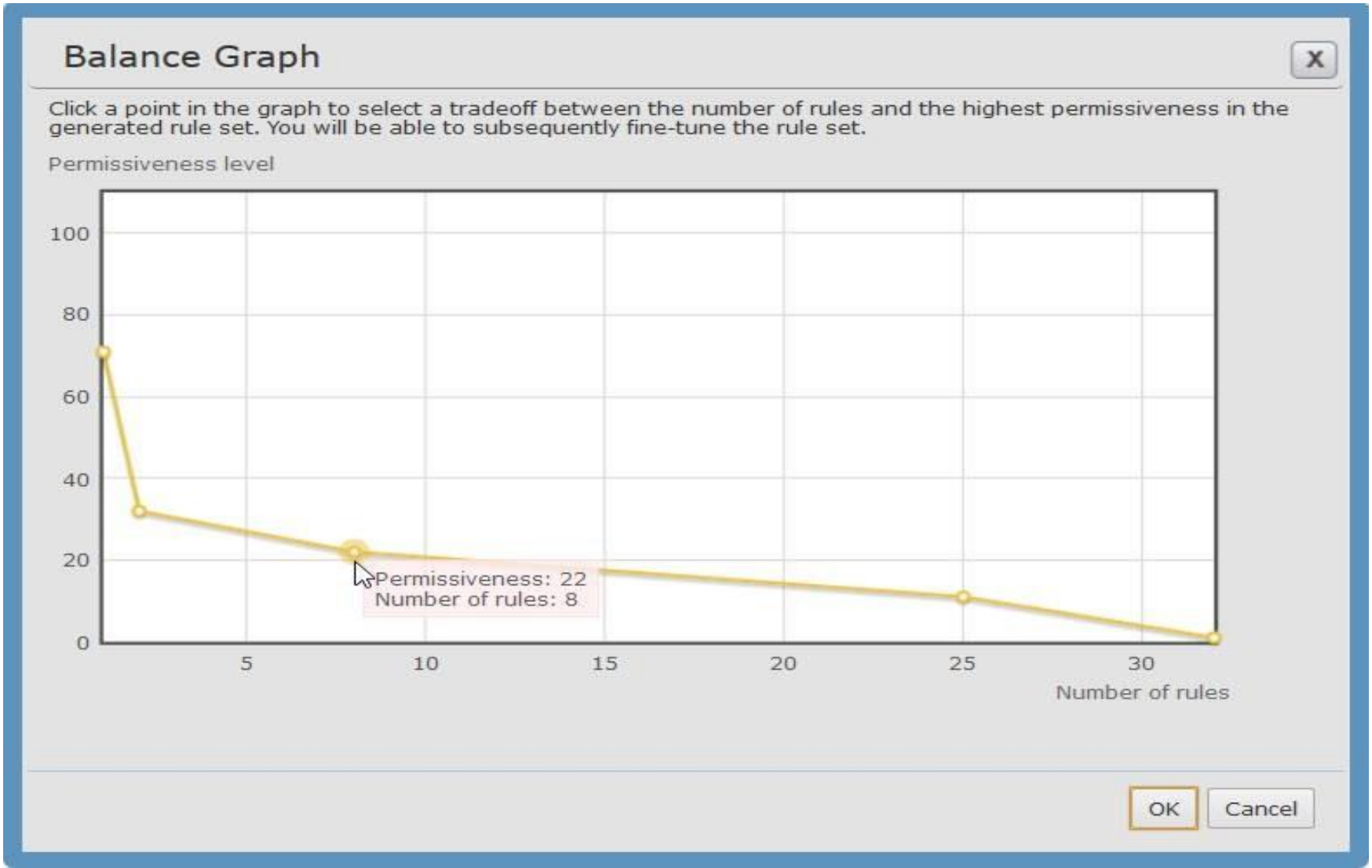
Expand a rule to replace it with several stricter rules (the more general rule is greyed out). The permissiveness score means:
* A rule with one source host, one destination host and one service has the smallest value - 1
* A rule with Source "ANY", Destination "ANY" and Protocol "ANY" has the highest value - 100

| Rule Name | Source | Destination | Protocol | Port | Hits | Permissiveness |
|---|---|---|---|---|---|---|
| Rule Rule.0 | 10.0.0.0/8 | 172.16.0.0/16 | Any | | 122 | 71 |
| Rule Rule.24 | 10.15.15.2/32 | 172.16.5.0/24 | Any | | 66 | 32 |
| Rule Rule.1 | 10.200.1.10/32 | 172.16.10.0/24 | Any | | 56 | 32 |
| Rule Rule.12 | 10.200.1.10/32 | 172.16.10.0/24 | TCP | 80 | 25 | 11 |
| Rule Rule.2 | 10.200.1.10/32 | 172.16.10.20/32 | Any | | 17 | 22 |
| Rule Rule.23 | 10.200.1.10/32 | 172.16.10.23/32 | TCP | 82 | 8 | 1 |
| Rule Rule.19 | 10.200.1.10/32 | 172.16.10.0/24 | TCP | 21 | 6 | 11 |
| Rule Rule.22 | 10.200.1.10/32 | 172.16.10.23/32 | TCP | 21 | 4 | 1 |
| Rule Rule.20 | 10.200.1.10/32 | 172.16.10.21/32 | TCP | 21 | 1 | 1 |
| Rule Rule.21 | 10.200.1.10/32 | 172.16.10.22/32 | TCP | 21 | 1 | 1 |

# Функционал SecureTrack

## Оптимизация правил и политик доступа (оптимизация ACL)

- В результате правило можно заменить на набор более «узких» правил, что повышает безопасность сети



# Функционал SecureChange

## Три ключевые функции

- Специализированная система обработки заявок на доступ
- Инструмент **превентивной** оценки рисков
- Механизм **контролируемого** автоматизированного внедрения сетевых правил и политик доступов

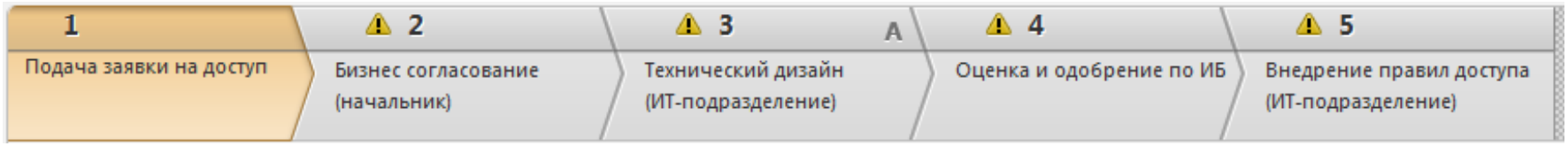
# Функционал SecureChange

## Система обработки заявок на сетевой доступ

### Общий функционал

Гибкий GUI-конструктор процессов (workflow) по шагам внесения изменений:

- Запрос,
- утверждение руководителем,
- Утверждение службой ИБ,
- Технический дизайн,
- Выполнение изменений,
- Проверка и подтверждение и т.п.



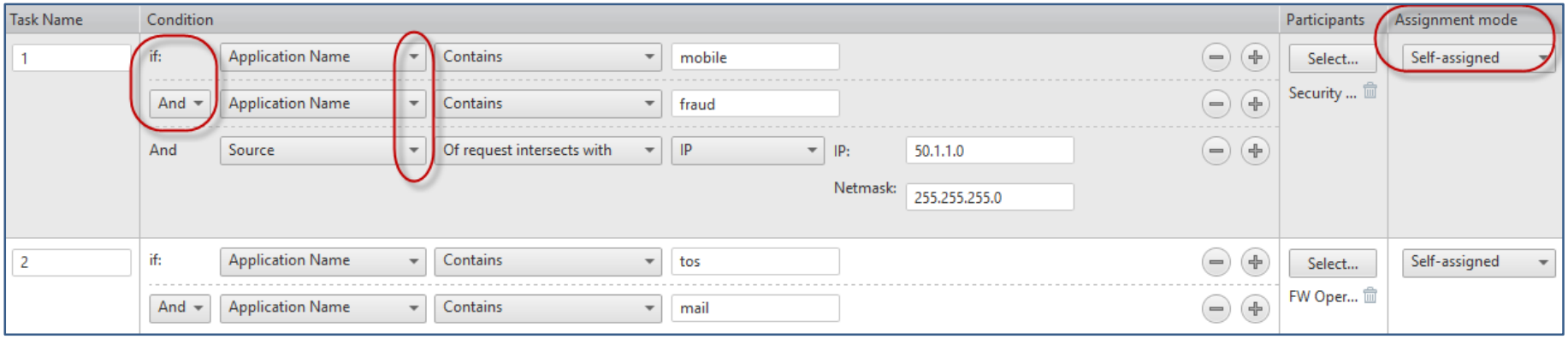
# Функционал SecureChange

## Система обработки заявок на сетевой доступ

### Общий функционал

Гибкий GUI-конструктор процессов (workflow) по шагам внесения изменений:

- Пять механизмов назначения и делегирования шагов
- Ролевая модель распределения задач
- Система ветвления условий («то – если»)
- Редактируемая конструкция SLA
- Web-интерфейс и интеграция с email
- Создание собственных конструкций, полей, условий



# Функционал SecureChange

## Система обработки заявок на сетевой доступ

## Специализированный функционал

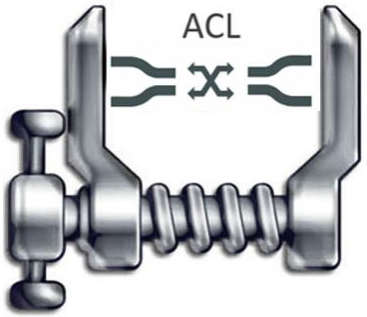
- Привязка шагов процессов к реальным техническим данным сети Заказчика

- Сопряжение «из коробки» с модулем Tufin Secure Track (не требуется интеграция)

В результате – на заданных шагах заявок по обработке доступа:

- Система оперирует объектами из баз МЭ, коммутаторов, маршрутизаторов и т.п.
- Система минимизирует и оптимизирует планируемое изменение (дизайн изменений)

**В чем отличие от систем Service Desk?**



# Функционал SecureChange

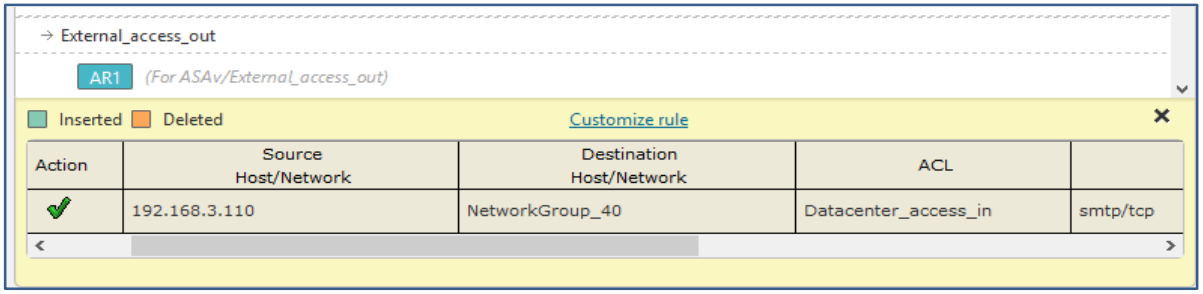
## Система обработки заявок на сетевой доступ

## Специализированный функционал

- Привязка шагов процессов к реальным техническим данным сети Заказчика

В результате – на заданных шагах заявок по обработке доступа:

- Система формирует конечное правило для каждого из сетевых устройств на языке ОС конечной системы и в графике
- Система оценивает риски для доступов до фактического внесения изменений
- Система может внедрять соответствующее изменение автоматически или используя механизм согласований и правок
- Система проверяет внедренные изменения



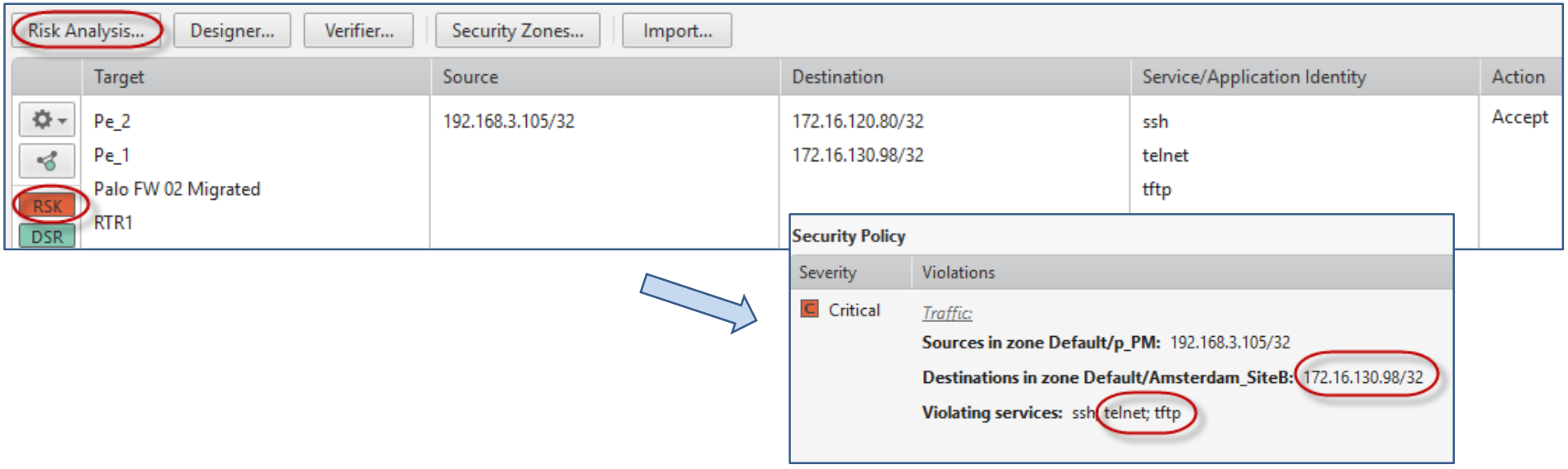

**В чем отличие от систем Service Desk?**

# Функционал SecureChange

## Инструмент превентивной оценки рисков

- Выявление попыток внесения изменений в сетевые устройства, противоречащих заданным политикам в компании (превентивно)

- Возможно создание подтвержденных исключений (при необходимости)

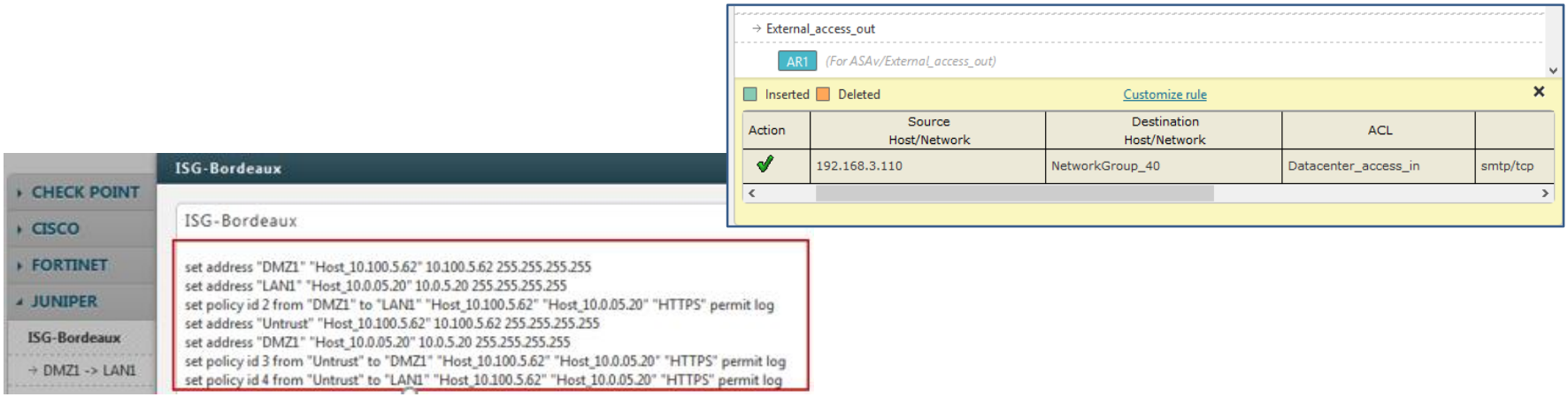


# Функционал SecureChange

## Механизм контролируемого автоматизированного внедрения правил

Модуль SecureChange обращается к модулю  SecureTrack и проверяет:

- Текущую структуру правил на каждом сетевом устройстве в пути
- Выбирает оптимальную структуру формирования изменения в каждом устройстве в соотношении того, что в устройстве уже есть
- Отображает планируемое изменение в графике и на языке ОС
- Предлагает механизмы правки и подтверждения изменения
- Самостоятельно может корректно прописать правило!

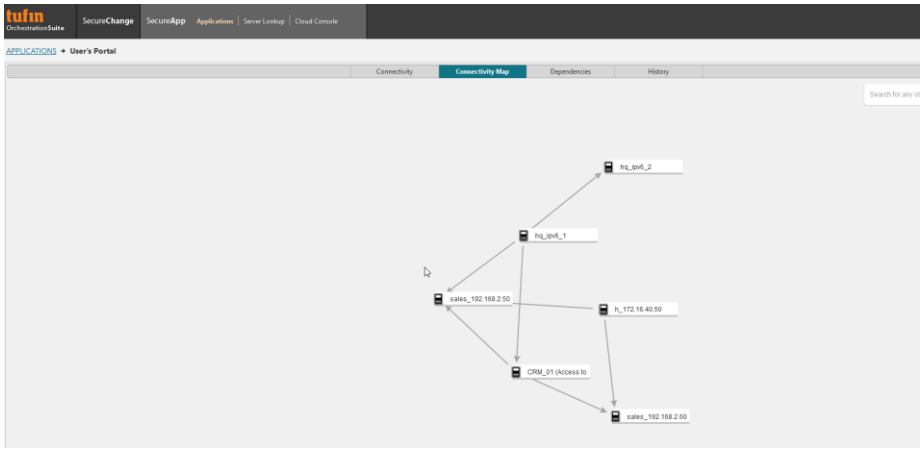


# Функционал SecureApp

## Основной функционал SecureApp

Модуль SecureApp обращается к модулю  SecureTrack и SecureChange и:

- Обеспечивает непрерывный контроль доступности приложений
- Управляет зависимостями между приложениями
- Фиксирует все изменения в приложении
- Контролирует планируемые изменения в конфигурации устройств на предмет влияния на доступность приложений
- Облегчает работу с вводом и выводом приложения в/из эксплуатации




# Спасибо за внимание!

NETWELL
УКРАЇНА