



tufin

Making Security Manageable

Tufin SecureChange: обработка заявок и автоматизация доступов

Александр Кушнарев,
Технический консультант,
Netwell Ltd.

Структура презентации

- ✓ Краткая информация о производителе
- ✓ Три ключевые функции SecureChange
- ✓ Функционал обработки заявок
- ✓ Инструмент превентивной оценки рисков
- ✓ Автоматизация изменений в доступах

Tufin Software Technologies - ключевой вендор Unified Firewalls Management



1700

клиентов
по всему
миру



Сочетание:

- Аналитика
- Автоматизация доступов
- Процессы



- Израильская компания
- В России более 7 лет



2012
EMERGING vendors

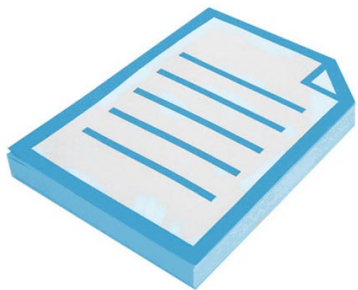


Deloitte.
Technology Fast50

Функционал SecureChange

Три ключевые функции

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



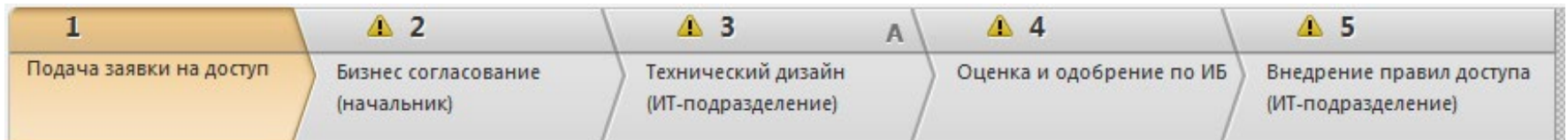
Функционал SecureChange

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

tufin

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

Task Name	Condition	Participants	Assignment mode
1	<p>if: Application Name Contains mobile</p> <p>And Application Name Contains fraud</p> <p>And Source Of request intersects with IP: 50.1.1.0 Netmask: 255.255.255.0</p>	Select... Security ...	Self-assigned
2	<p>if: Application Name Contains tos</p> <p>And Application Name Contains mail</p>	Select... FW Oper...	Self-assigned

Функционал SecureChange

Система обработки заявок на сетевой доступ

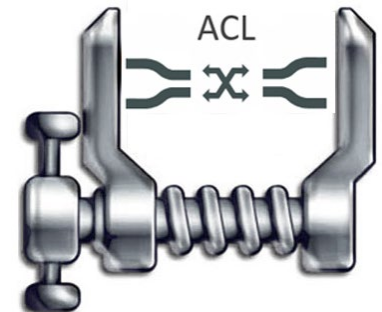
Специализированный функционал

- 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

Инструмент превентивной оценки рисков

- Выявление попыток внесения изменений в сетевые устройства, противоречащих заданным политикам в компании (превентивно)
- Возможно создание подтвержденных исключений (при необходимости)

The screenshot displays the 'Risk Analysis...' tab in the SecureChange interface. A table lists the configuration details for 'Palo FW 02 Migrated', showing a risk level of 'RSK' (circled in red) and a destination IP of '172.16.130.98/32'. A detailed view of the 'Security Policy' shows a 'Critical' violation (marked with a red 'C') for traffic from source '192.168.3.105/32' to destination '172.16.130.98/32' (circled in red). The violating services are listed as 'ssh, telnet; tftp', with 'telnet; tftp' circled in red. A blue arrow points from the table row to the detailed policy view.

Target	Source	Destination	Service/Application Identity	Action
Pe_2	192.168.3.105/32	172.16.120.80/32	ssh	Accept
Pe_1		172.16.130.98/32	telnet	
Palo FW 02 Migrated			tftp	

Severity	Violations
Critical	<i>Traffic:</i> Sources in zone Default/p_PM: 192.168.3.105/32 Destinations in zone Default/Amsterdam_SiteB: 172.16.130.98/32 Violating services: ssh, telnet; tftp

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!

The screenshot displays the configuration for a rule named 'External_access_out' in the SecureChange interface. The rule is associated with the device 'AR1' (For ASA/External_access_out). The rule is currently in an 'Inserted' state. The configuration table shows the following details:

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

Below the configuration table, a list of commands for the device 'ISG-Bordeaux' is shown, enclosed in a red box:

```
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
```



tufin

Making Security Manageable

СПАСИБО ВАМ!

Netwell Ltd.
info@netwell.ru,

+7 (495) 66 239 66