



**tufin**

Making Security Manageable

## Ключевые задачи управления сетевым доступом

Александр Кушнарев,  
Технический консультант,  
Netwell Ltd.

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

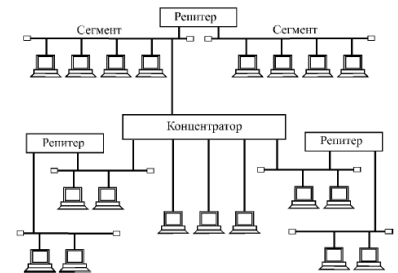
# Когда актуально?

- ✓ 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)



## 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)

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		

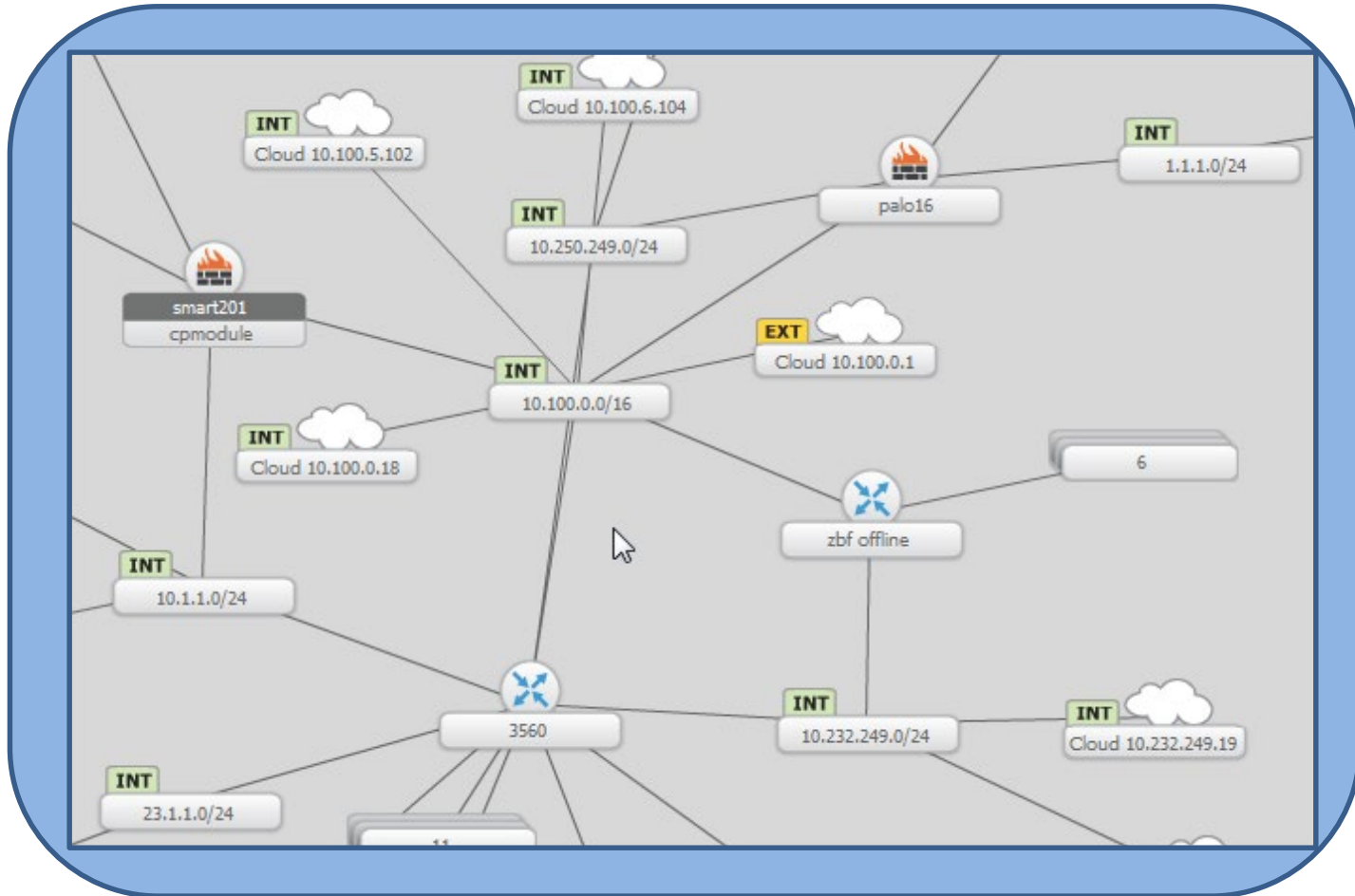
Стало «разрешить»      Сейчас такие адреса

Пару минут назад в правилах 2, 3 и 4

Сейчас в правилах 2, 3 и 4



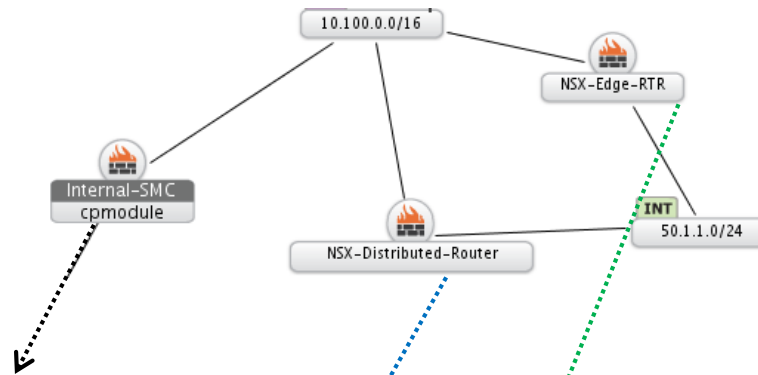
# Сетевая топологическая карта



✓ 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	<a href="#">Web01 - Network adapter 2</a>	<a href="#">ipset_range</a>	<a href="#">test_icon</a>	<a href="#">MGMT-PortGroup</a>	<a href="#">DC_test2</a>	<a href="#">MGMT</a>	<a href="#">MGMT-PortGroup</a>	<a href="#">none</a>	<a href="#">Data Recovery Appliance</a>	<a href="#">DNS</a>	<a href="#">UDP_500</a>
----	---	-----------------------------	---------------------------	--------------------------------	--------------------------	----------------------	--------------------------------	----------------------	---	---------------------	-------------------------

Такого доступа не будет, сработает правило № 53

53	Partially Shadowed	Default Rule	* Any	* Any	* Any
----	--------------------	--------------	-------	-------	-------

# Единая контролируемая точка внесения изменений

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

ISG-Bordeaux

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 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

**Policy Type:**  
Risk Management

**Rule details**

No.	Name	Source	Destination	Service	Application and User
1	Telnet restrictions <b>Description:</b> Запрещено использование telnet-приложений техподдержке для серверов в DMZ	<input type="radio"/> All sources <input type="radio"/> Network Object Defined in: CSM Object Name: <input checked="" type="radio"/> Custom Network Address: 192.168.5.0 Network Mask: 255.255.255.0 <input type="checkbox"/> Negate	<input type="radio"/> All destinations <input checked="" type="radio"/> Network Object Defined in: SecureTrack Object Name: DMZ <input type="radio"/> Custom Network Address: 0.0.0.0 Network Mask: 0.0.0.0 <input type="checkbox"/> Negate	<input type="radio"/> All services <input type="radio"/> Service Defined in: CSM Object Name: <input checked="" type="radio"/> Custom Protocol: TCP Port: 23 <input type="checkbox"/> Negate	<input type="radio"/> All applications <input checked="" type="radio"/> Application/s: ms-telnet, putty, Ir (separated by ",") <input type="radio"/> All users <input checked="" type="radio"/> User/s: helpdesk (separated by ",")

- ✓ 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

The screenshot shows 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 is displayed in a table with the following columns: Action, Source Host/Network, Destination Host/Network, ACL, and an empty column. The rule configuration is as follows:

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

Below the table is a horizontal scrollbar. The interface also includes a 'Customize rule' link and a close button (X) in the top right corner of the table area.

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



**tufin**

Making Security Manageable

СПАСИБО ВАМ!

Александр Кушнарев,  
Технический консультант,  
Netwell Ltd.

[akushnarev@netwell.ru](mailto:akushnarev@netwell.ru),

+7 (495) 66 239 66