Целевое управление доступом в сети: решение Tufin TOS

- Состав решения,
- Для чего нужно?
- Ценность для ИТ и ИБ
- Техническая демонстрация

Максим Аношко,
manoshko@Netwell.com.ua
Технический консультант,
Netwell-Ukraine.
+38 044 359 07 79

Tufin Software Technologies - ключевой вендор Unified Firewalls Management

1500

клиентов по всему миру

Сочетание:

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

- Израильская компания
- Автоматизация правил доступа

SC MAGAZINE BEST BUY

Info Security Products Guide 2013 GLOBAL EXCELLENCE BRONZE

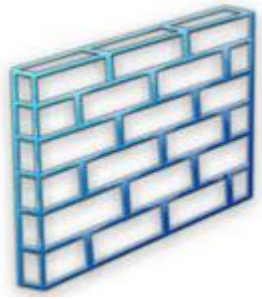
2012 EMERGING vendors

NETWORK computing AWARDS 2012 FINALIST

SC MAGAZINE AWARDS 2012 EUROPE

Deloitte. Technology Fast50

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

NETWELL

Порядок подключения, протоколы (примеры)

Juniper

* M, MX-routers,
* Services Gateway SRX,
* Платформы NetScreen,
* J-серия Service Routers,
* VPN SSL SA

- SSH, Telnet – опрос,
- Syslog – по изменению

- SSH, Telnet – опрос

*** Центр управления NSM Central Manager**

- **NSM API (TCP 8443)**
- **По изменению**

Stonesoft

* Большинство устройств

*** Центр управления Stonesoft Management Center**

- **REST (TCP 8082), опрос**

Cisco

* Firewalls ASA, PIX, FWSM
* XR IOS – устройства
* Cisco Nexus-коммутаторы
* Общие коннекторы Router, Switch
* Catalyst, Ironport ESA, CSS

*** Центр управления CSM**

- SSH, Telnet – опрос,
- Syslog – по изменению

- SSH, Telnet – опрос
- **SSL, TCP 443**

Порядок подключения, протоколы

F5

* Устройства BIG-IP,

*** Центр управления BIG-IP LTM**

- SSH, Telnet – опрос
- **SSH, Telnet – опрос**

Кроме того – поддерживается (не весь перечень):

- Учет влияния NAT-правил: CheckPoint, Cisco, Juniper, F5
- Проверка PCI DSS: CheckPoint, Juniper, Cisco, Fortinet, Palo Alto, Stonesoft
- Сравнение правил – все устройства
- Показ учетных записей – CheckPoint, Cisco, Fortinet, Juniper, Palo Alto
- Топология – все устройства
- Динамическая топология - CheckPoint, Cisco, Fortinet, Juniper, Palo Alto
- SNMP – для «очень активных» изменений

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

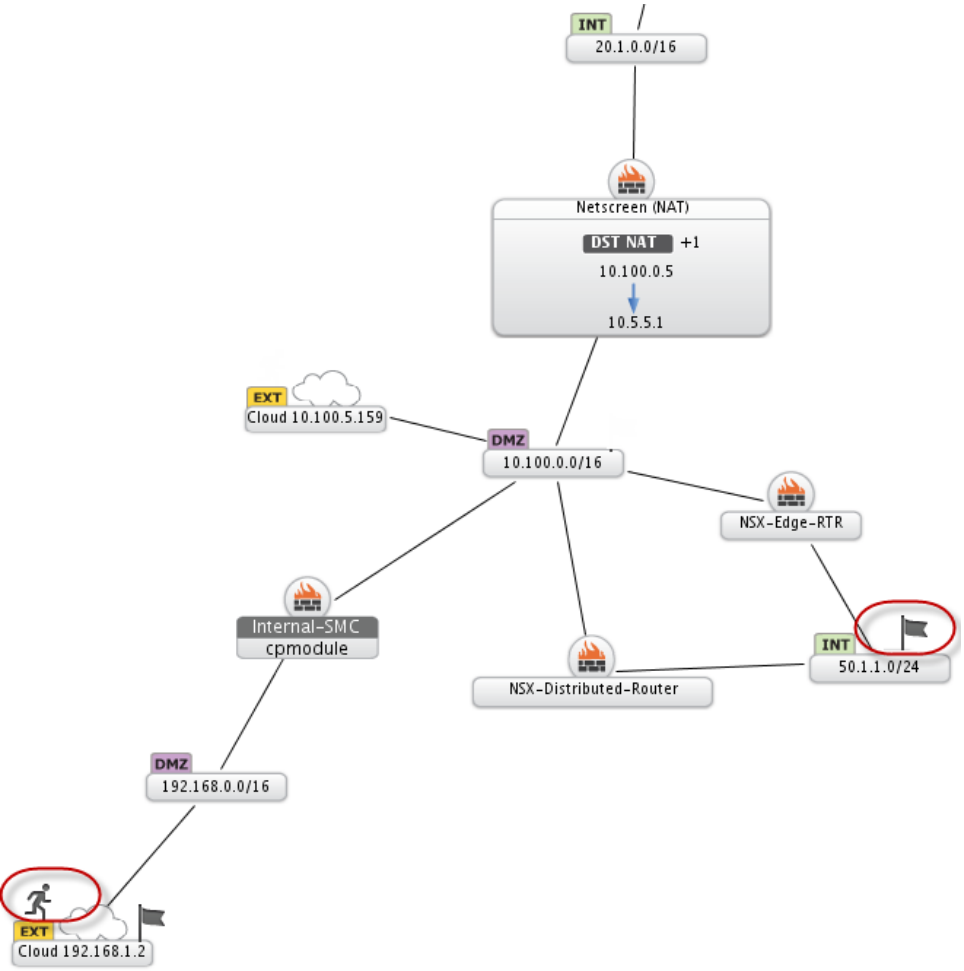
Компьютер пользователя (для некоторых МЭ)

Набор политик

tufin

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

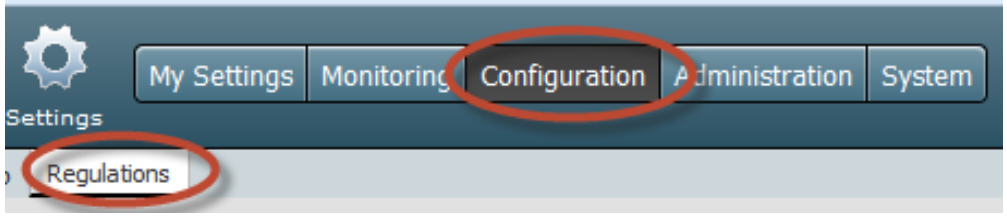
Хост

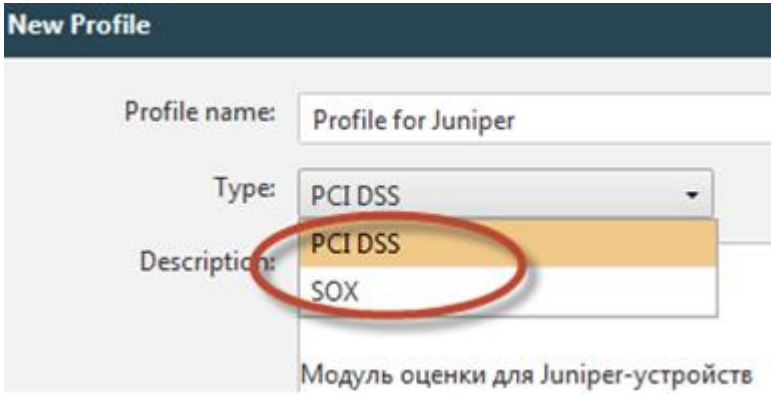
Приложение

Функционал проверки соответствия PCI DSS

Формирование индивидуального профиля

- ✓ Модуль контроля изменений содержит функционал оперативной оценки соответствия:
  - ✓ Задается профиль с выбором PCI DSS или Sox
  - ✓ Производится определение и выборка: внутренних подсетей, приложений и сервисов, беспроводных зон доступа и др.
  - ✓ Запускается оценка – результат на консоли или в виде отчета





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 то в этом виноват?» - когда что-то случается (ИТ и ИБ)

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

Ключевые блоки функционала Tufin TOS:

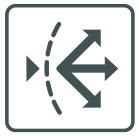
работа с сетевым оборудованием

Интерактивная сетевая карта

Анализ изменений в реальном времени

Единая точка внесения изменений

Оптимизация баз правил



Распределение ответственности

Соблюдение требований безопасности

Ценность для IT-специалистов

✓ Средство организации и поддержки порядка в ACL:

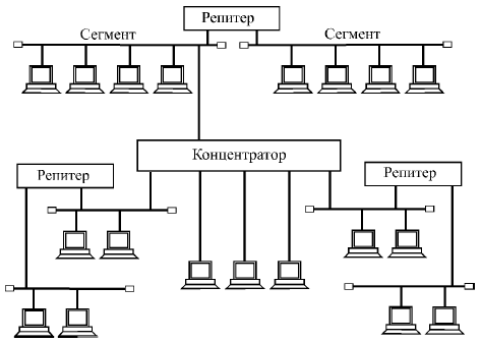
- Дублирующие, перекрывающие, неиспользуемые объекты и правила
- Фактическое использование правил – оптимизация

✓ Единая точка анализа и продвижения правил доступа:

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

✓ Оперативный анализ доступов любой сложности:

- Влияния 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

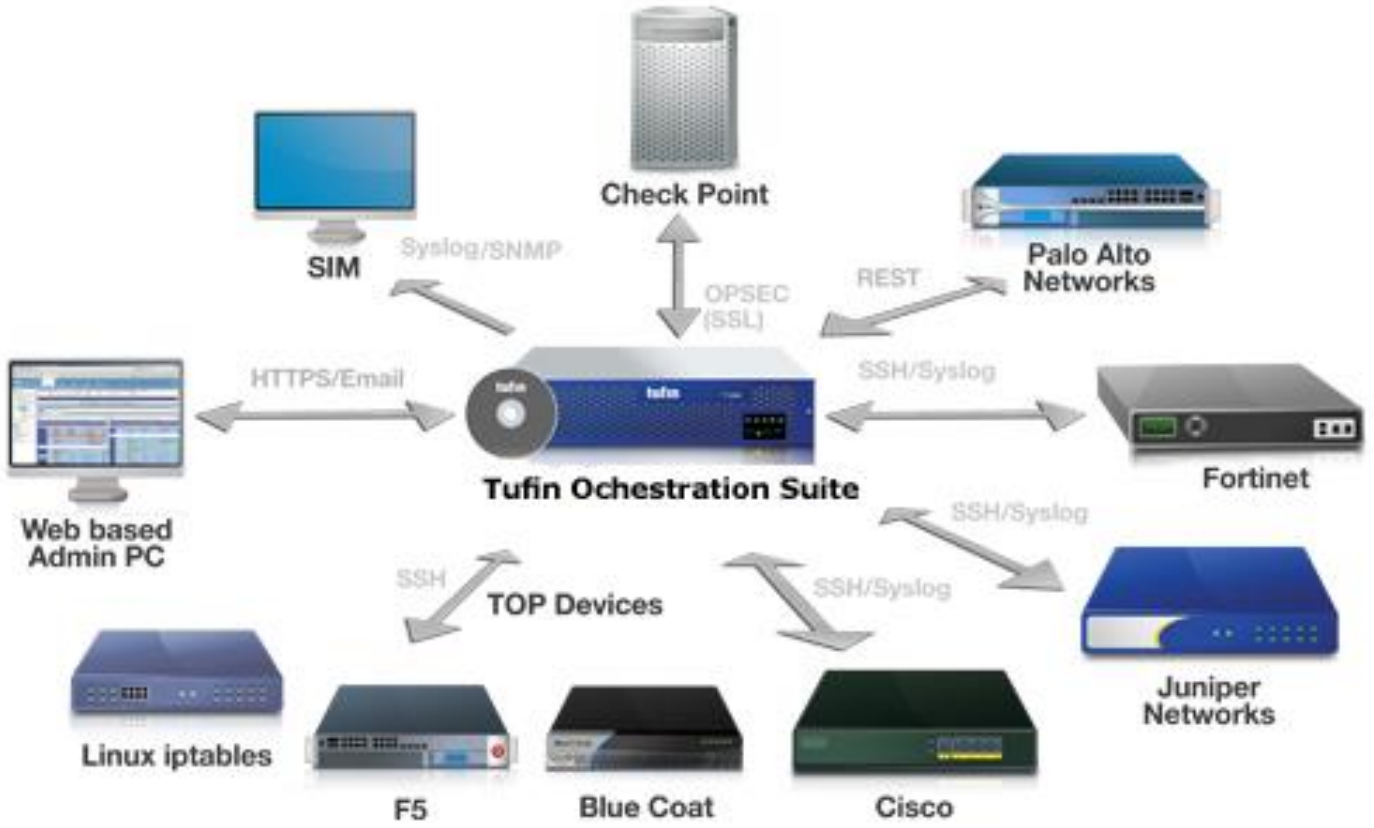
✓ Фиксация и формализация действий по доступу:

- 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

Спасибо за внимание!



NETWELL УКРАЇНА