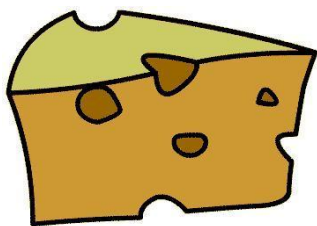


Управление Безопасностью

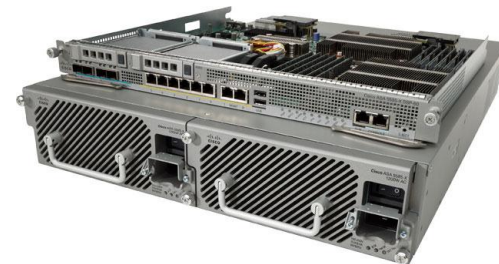
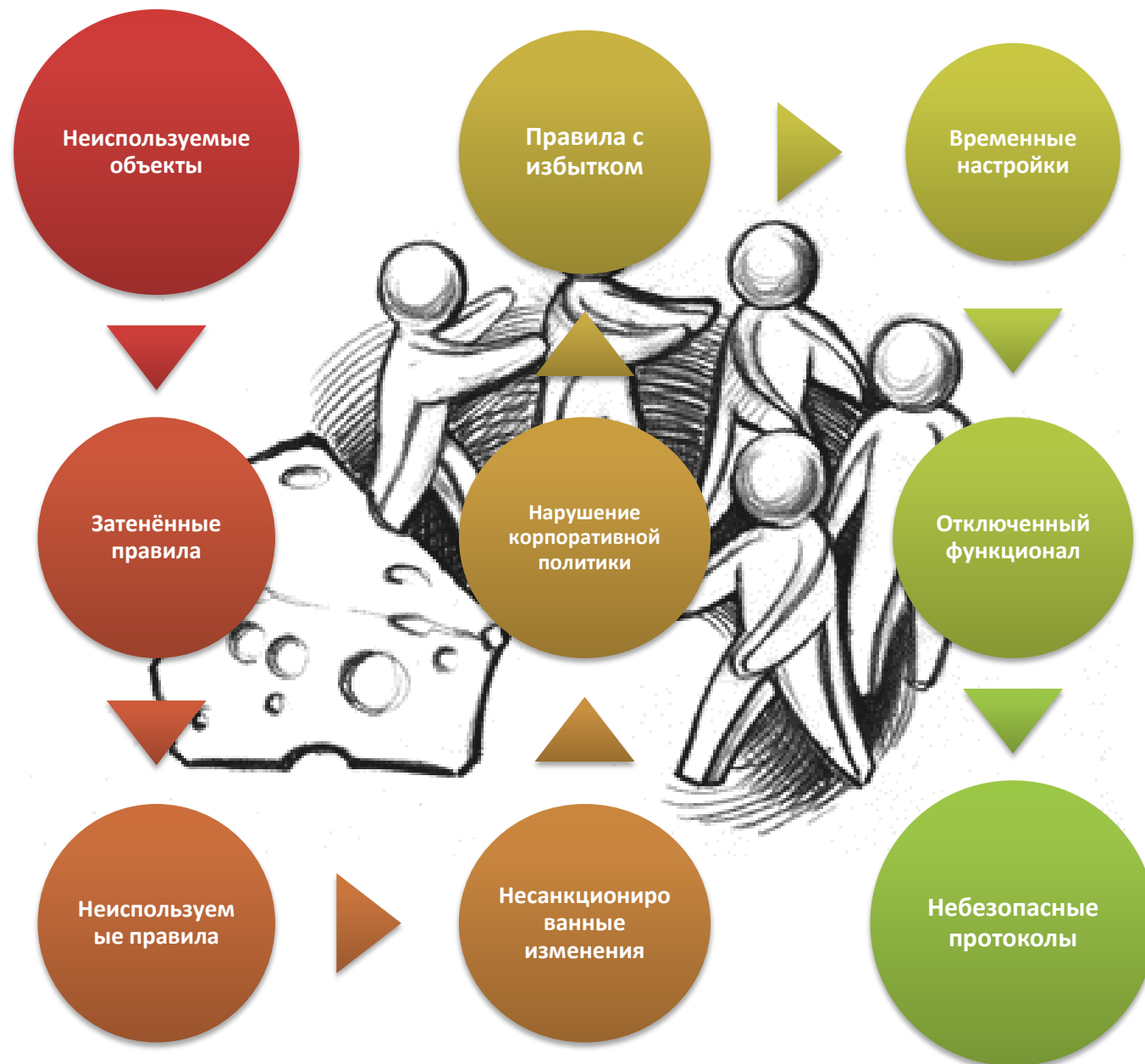
Pete Kuzeev, Security Expert, RRC Moscow



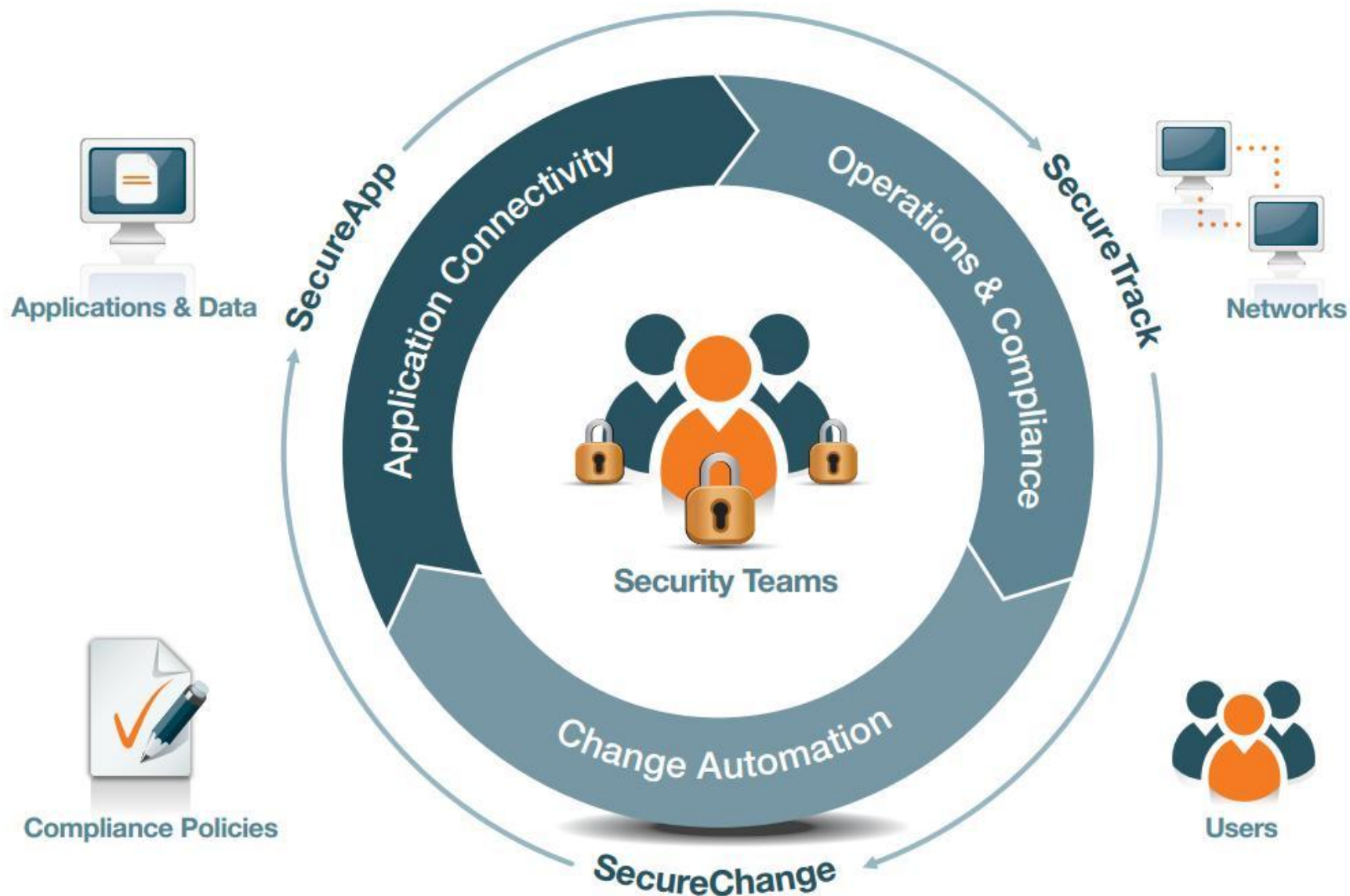
tufin

Эффективность защиты – это точность и скорость ответов на поставленные вопросы

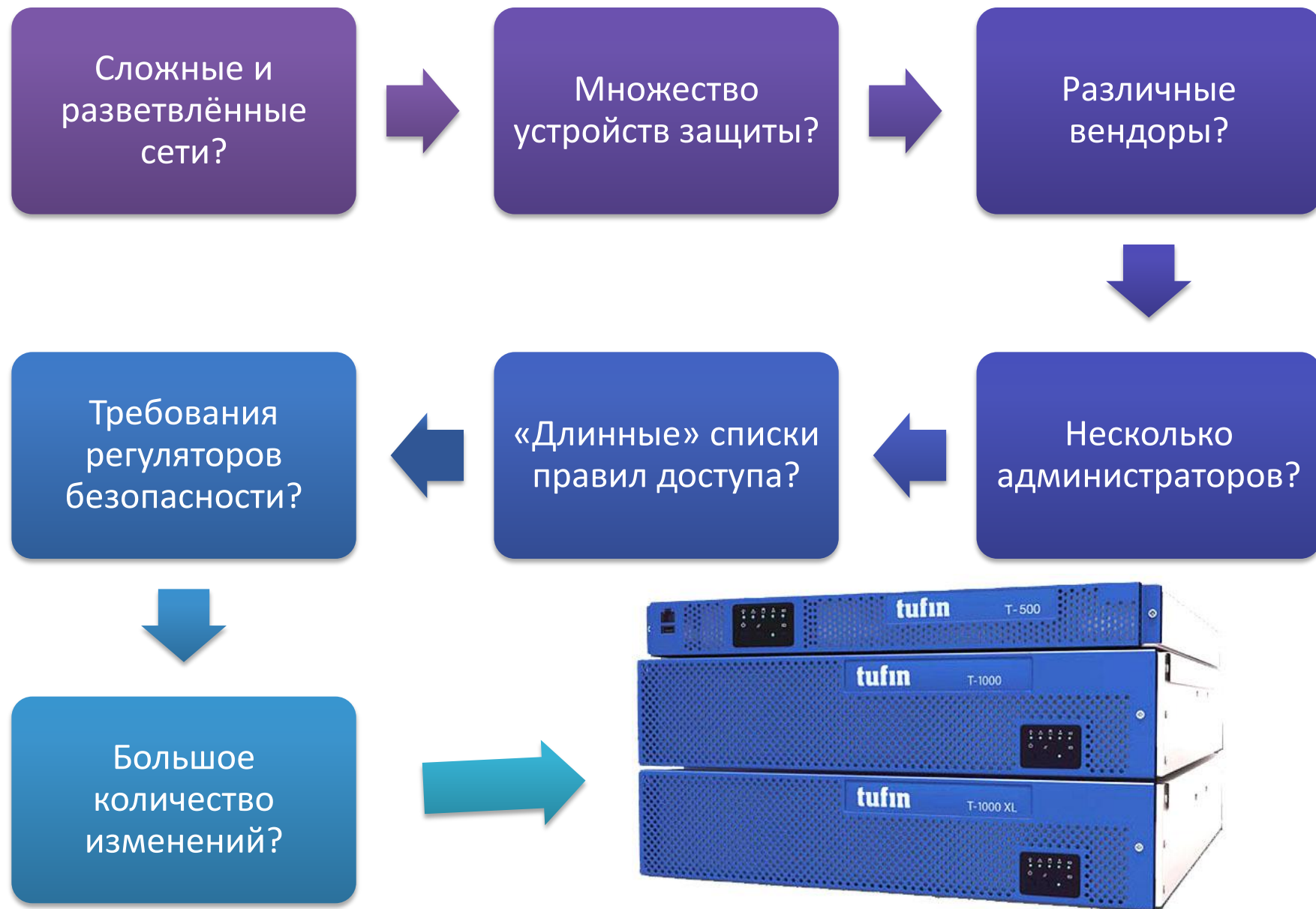
Почему именно сыр?



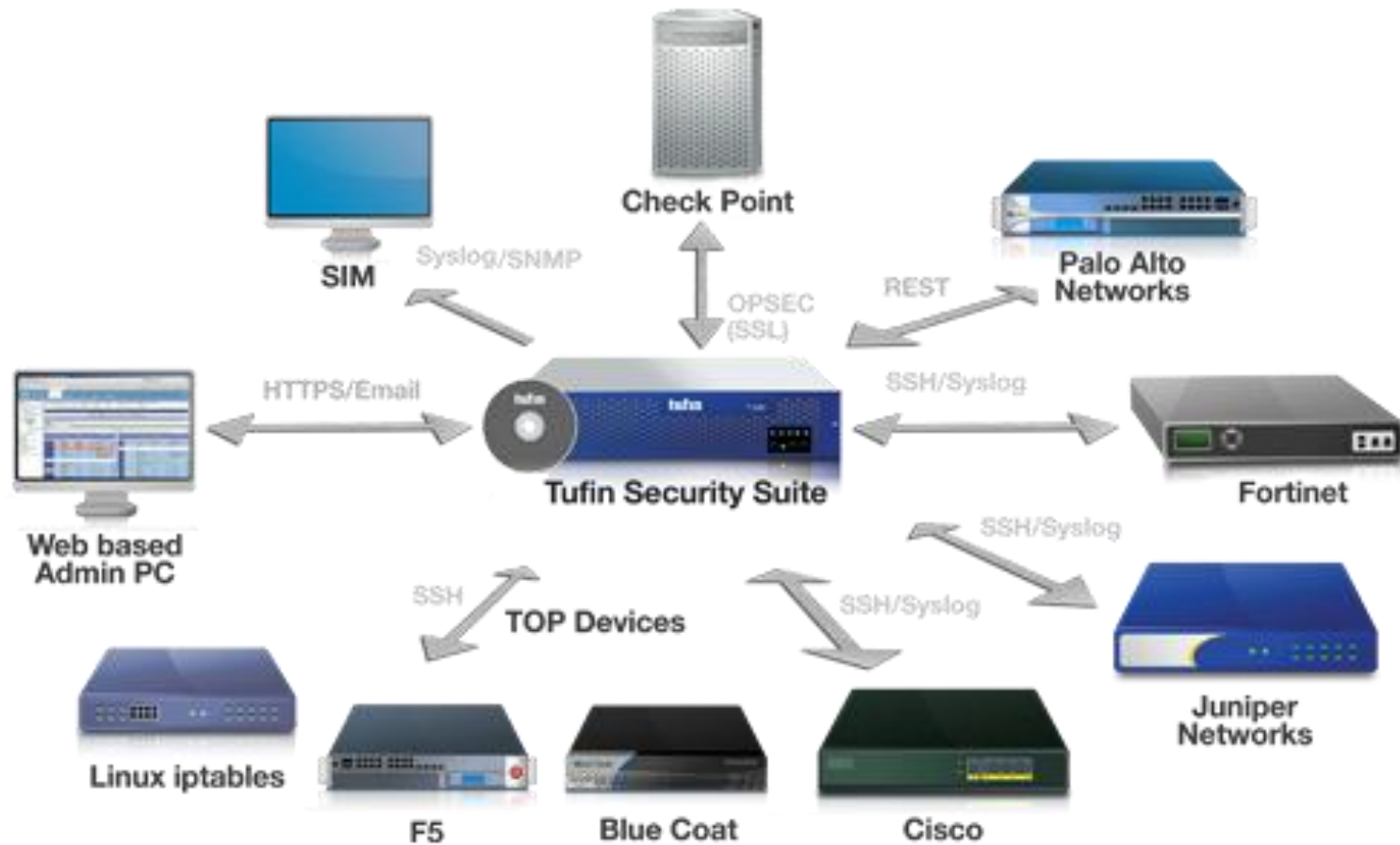
Что такое Tufin сегодня?

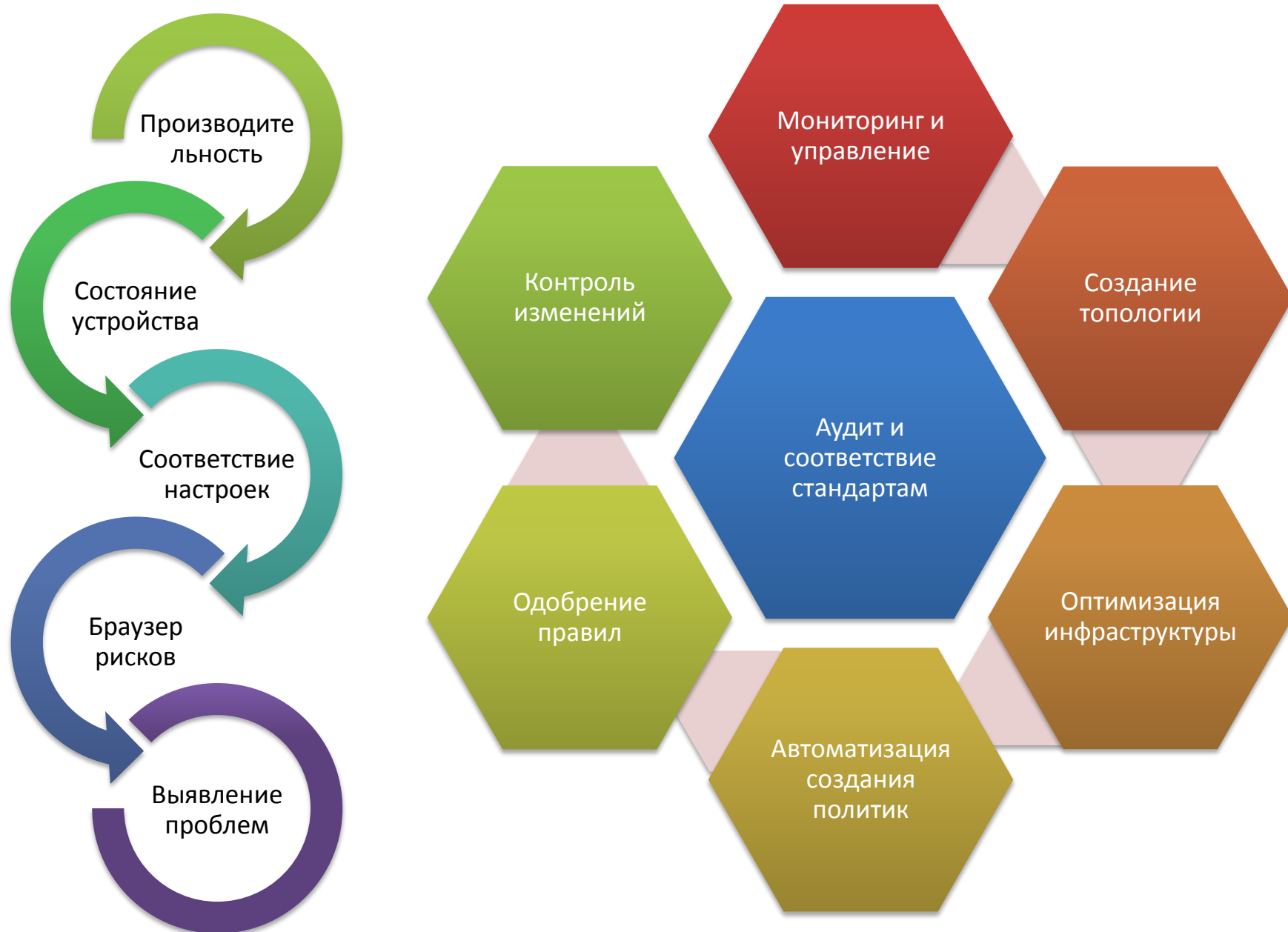


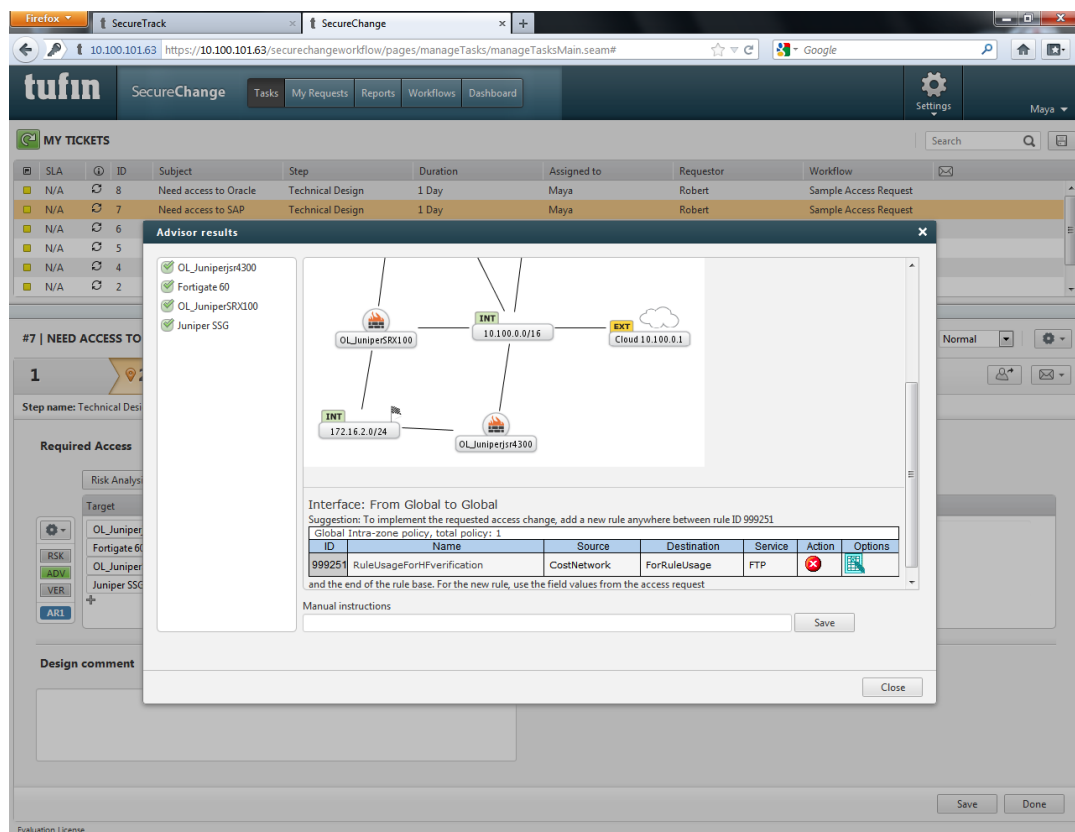
Кому Tufin необходим?



Как это работает?







Отслежива
ние SLA

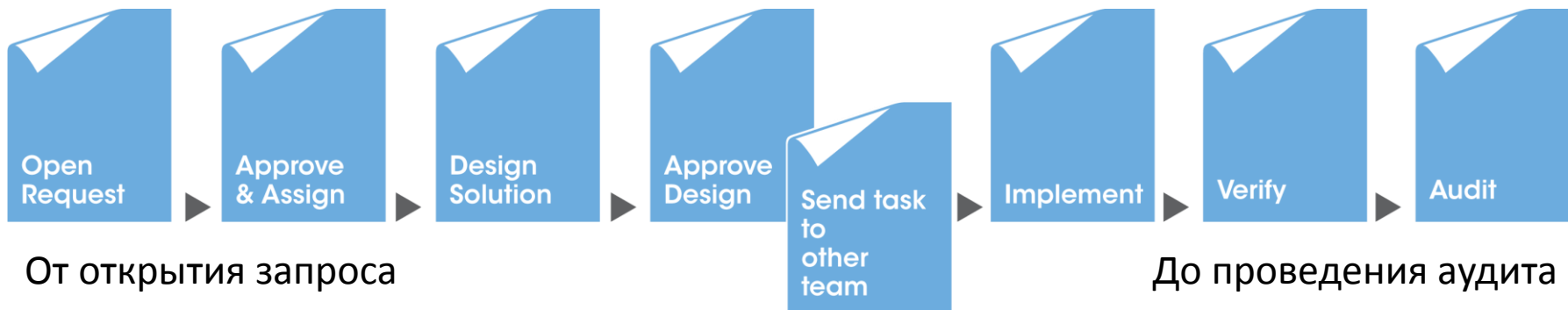
Дизайнер
политик

Управление
процессами

Анализ
рисков

Возможности
интеграции

Автомати
ческая
проверка
запросов



Firefox Mozilla Firefox Start Page

tufin SecureChange Basic SecureApp Settings Username

APPLICATIONS LIST → LAB MANAGER

Connectivity History

New Connection Revert Save Connection Sort By: Date Filter By Create a Ticket...

Name	Source	Service	Destination	Comment	Status
Lorem Ipsum is the printing	Win LM R&D	HTTPS	Win Vcenter Win Vcenter-2 (Info)	Lorem Ipsum is simply dummy text of the printing and typesetting industry.	Connection Monitoring: OFF ON 1
Lorem Ipsum is the printing	Win LM R&D	HTTPS	Add Servers or Any	Lorem Ipsum is simply dummy text of the printing and typesetting industry.	Connection Monitoring: OFF ON --
Default Name	Win LM ESX25	HTTPS	Win Vcenter ESX4 ESX5 LDAP: Serve... (Info)	Lorem Ipsum is simply dummy text of the printing and typesetting industry.	Connection Monitoring: OFF ON --

Confidential - Not for Distribution

Resources

- Services
- Users
- Applications
- Lab Manager
 - DB-Post
 - Guliver_123
 - Semion_rules Kokik...
 - Test-M
 - Win Vcenter 2
 - DB2-34 10.12.14.52/24
 - Win Vcenter Huki... 102.122.142.932-123...
 - DB2-3 10.12.14.52/24
 - Win Vcenter230 103.124.145.934/32
 - Win Vcenter5 10.12.14.93/24
 - Win Vcenter5

Корпоративные приложения

Пользователи приложений

Отдел безопасности

Политики и устройства

tufin SecureTrack Home Compare Analyze Audit Report Network **Topology** Zones Settings

Search: [] Synchronize Add Generic Device

Interfaces **Routing Table**

Network	Interface	Gateway
1.1.1.1/24		5.5.5.5
1.1.1.1/24		5.5.5.5
1.1.1.1/32	ethernet0/1	2.2.2.2
10.10.10.103/32	bgroup0	10.10.10.2
10.100.104.97/32	bgroup0	8.8.8.1
11.11.11.0/24	ethernet0/0	172.16.2.201
12.12.12.12/32	ethernet0/0	172.16.2.166
14.14.0.0/16	ethernet0/0	172.16.2.201
55.55.55.55/32	ethernet0/0	172.16.2.159
7.7.7.0/24	ethernet0/0	172.16.2.166
default gateway	ethernet0/0	10.100.0.1

Save Cancel

Licensed to Customer 1 Attention Required Thu, 2 Feb 2012 17:38

Таблицы
маршрутов
одним
кликом



Добавление
устройств



Определение
периметров

RRC Сравнение и копирование конфигураций

Копия
конфигурации
для каждой
реvisions

Поиск
изменений

Корреляция
изменений к
устройствам

Revision History - CMA-Hamburg - 14 revisions during the last 1000000 hours

Revision	Action	Date	Time	Administrator	Installed on	GUI client	Audit log	Policy package	Global policy	Ticket ID	Comment
14	📄	Fri, 07 Mar 2008	18:16:14	John	-	ruvilap2	494	policy_a	-	CHG1-00374	interesting
13	📄	Thu, 06 Mar 2008	22:30:42	John	-	ruvilap2	453	policy_a	-	-	Click to edit...
12	📄	Thu, 06 Mar 2008	22:17:37	John	-	ruvilap2	450	policy_a	-	-	Click to edit...
11	📄	Thu, 06 Mar 2008	20:38:12	John	cpmodule	ruvilap2	436	policy_a	-	-	Click to edit...
	📄	Thu, 06 Mar 2008	20:37:12	John	-	ruvilap2	431	policy_a	-	-	Click to edit...
10	📄	Tue, 04 Mar 2008	21:34:50	John	-	ruvilap2	420	policy_a	-	-	Click to edit...

Filter View Policy Compare Generate Report

Comparison

Rules Objects Global Properties Legend: Deleted Inserted Modified Modified rule fields

Security Address Translation

policy_a policy_a

CMA-Hamburg - Revision 13 - John - Thu, 06 Mar 2008 22:30:42

Id	Object	Policy	Action	Comment
5	SecureTrack	cpmodule	Any	TCP FW1_ica_pull TCP FW1_lea TCP CPMI accept
6	Internal	AccountsDB	Any	TCP telnet drop
7	LimitedAccounts	PatentDB	Any	https drop

CMA-Hamburg - Revision 14 - John - Fri, 07 Mar 2008 18:16:14

Id	Object	Policy	Action	Comment
5	SecureTrack	cpmodule	Any	TCP FW1_ica_pull TCP FW1_lea TCP CPMI accept
6	Customer-1	CreditInfo SpecialAccount	Any	TCP sqlnet1 accept
7	Internal	AccountsDB	Any	TCP telnet drop
8	LimitedAccounts	PatentDB	Any	https drop

Evaluation license (for Evaluating Customer) expires in 14 day(s)

Fri, 3 Feb 2012 14:15

EN 100%

23:48

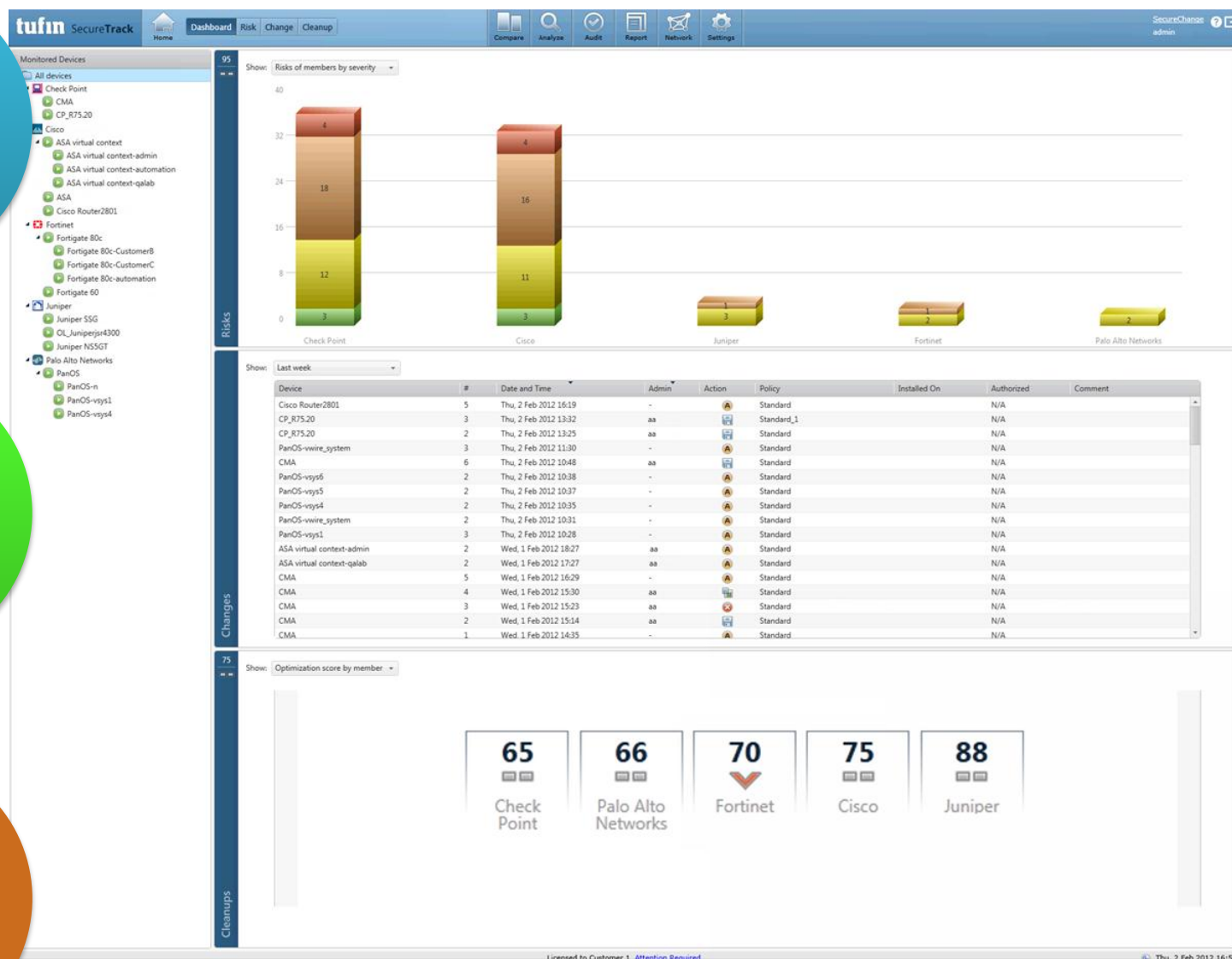
Текущий
уровень
рисков

Исторические
тенденции

Установка
политик и
приоритетов

Рекомендова
нные
заплаты

Глобально
или для
шлюза



Analysis Queries Automatic Policy Generator

New job stage 1
Select permissive rule for replacement

From a device policy, select an overly permissive rule that should be replaced with a set of tighter rules allowing only actual business traffic, and click Next.

ASA - Revision 2 - Policy 'Standard' - enable_15 - Thu, 03 Feb 2011 12:01:34

Permissiveness	#	Action	Source Host/Network	Destination Host/Network	ACL	Service	Log Level Interval	Description
61	1	✗	192.0.0.0	192.168.2.0/255.255.255.0	outside_access_in	ip		
83	2	✓	Any	Any	outside_access_in	surfing		marina
70	3	✓	192.0.0.0	Any	outside_access_in	syslog/udp		
41	4	✓	192.0.0.0	192.168.2.0/255.255.255.0	outside_access_in	http/tcp		http://www.yynet.co.il/articles/0,7340,L-4021537,00.html
34	5	✓	Group:NET_GRP	192.168.2.0/255.255.255.0	outside_access_in	ftp/tcp data/tcp ldap/tcp ldaps/tcp ssh/tcp telnet/tcp syslog/udp		lalalala1 zzzz ticket86 rule-specific comment < < < < 12345678 test rule CR29282 fgdgdfg 4 1111 rule-specific comment < < < < 12345678 test rule CR29282 test comment 4 wwwwww dddddd lalalala1 zzzz ticket86 rule-specific comment < < < < 12345678 test rule CR29282 test comment 4 fgdgdfg 4 http://www.yynet.co.il/articles/0,7340,L-4021537,00.html 1111 rule-specific comment < < < < 12345678 test rule CR29282 test comment 4 wwwwww dddddd test comment 4 4
54	1	✓	192.168.2.0/255.255.255.0	Any	inside_access_in_2	surfing		
100	2	✗	Any	Any	inside_access_in_2	ip		
50	1	✓	192.0.0.0	192.NET_16	global_access_2	gre/ip		
32	2	✓	Group:NET_GRP	192.168.2.0/255.255.255.0	global_access_2	telnet/tcp		

Сравнение изменений с политикой соответствия



Оповещение в случае нарушения



Оповещение владельцев сервисов

Оптимизация базы правил

Анализ логов



Сравнение с базой правил



Предложение по оптимизации

SecureTrack - Tufin Technologies - Windows Internet Explorer

https://SecureTrack

SecureTrack - Tufin Technologies

tufin SecureTrack Compare Analyze Audit Report Configure Help Logout

General Reports Business Ownership Reports Repository

Rule Usage Report - 'Docklands Rule Usage'

Results Complete Edit Report Period

Most-used rules - 2 of 15 (top 10%) [back to SMC-Docklands](#)

NO.	HITS	FIRST HIT	LAST HIT	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
5	123 (38%)	Wed, 05 Dec 2007 00:00	Thu, 06 Dec 2007 08:00		Host_192.168.1.120 123 (100%)	Docklands 123 (100%) Paris 0 (0%)	* Any	udp snmp 123 (100%)	accept	Log	* Any	* Any	
7	111 (34%)	Wed, 05 Dec 2007 00:00	Thu, 06 Dec 2007 04:00		Host_9.3.3.10 0 (0%) Host_9.3.3.11 111 (100%) Host_7.7.7.7 0 (0%)	Host_7.1.1.100 40 (36%) Host_7.1.1.101 71 (64%) Host_7.1.1.102 0 (0%)	* Any	TCP http 111 (100%) TCP ftp 0 (0%)	accept	Log	* Any	* Any	CHG1-008355

Least-used rules - 2 of 15 (bottom 10%) [back to SMC-Docklands](#)

NO.	HITS	FIRST HIT	LAST HIT	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
12	1 (0%)	Wed, 05 Dec 2007 01:00	Wed, 05 Dec 2007 01:00		Net_192.168.1.0 1 (100%) Net_7.0.0.0 0 (0%)	Host_9.3.3.10 0 (0%) Host_9.3.3.11 1 (100%) Host_9.3.3.9 0 (0%) Host_9.3.3.50 0 (0%) NAT_Host_9.99.99.10 0 (0%) NAT_Host_9.99.99.11 0 (0%) NAT_Host_9.99.99.9 0 (0%)	* Any	* Any	drop	Log	* Any	* Any	CHG1-008360
1	4 (1%)	Wed, 05 Dec 2007 00:00	Thu, 06 Dec 2007 03:00		Net_192.168.1.0 4 (100%)	all firewalls 4 (100%)	* Any	TCP ssh 4 (100%)	accept	Log	* Any	* Any	CHG1-008334 CHG1-0090113

Unused rules - 4 of 15 [back to SMC-Docklands](#)

NO.	HITS	FIRST HIT	LAST HIT	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
2	0				Net_192.168.1.0	SMC_Docklands	* Any	TCP ssh	accept	Log	* Any	* Any	CHG1-0090112
4	0				Host_192.168.1.120	SMC_Docklands	* Any	TCP FW1_ica_pull	accept	Log	* Any	* Any	
							* Any	TCP FW1_lea	accept	Log	* Any	* Any	

John Denver (admin) Time on Server: Mon, 29 Dec 2009 22:09

Неиспользуемые
правила



Неиспользуемые
объекты



Статистика по
правилам

tufin SecureTrack Compare Analyze Audit **Report** Configure

General Reports Business Ownership Published Reports

Baseline Settings Compliance Report - 'Baseline Settings Compliance Report 17/02/2008'

Results Complete

Baseline Settings Compliance Report - 'Baseline Settings Compliance Report 17/02/2008'

Generated on 10 Nov 2007, 21:00:55 by John Denver
Report Time: Sun, 17 Feb 2008, 13:13

Baseline Management: HamburgCMA

Compliance Summary

Management Server	Compliant	Not Compliant
SportsGoodsCMA		x
Citycabs	v	
SuperEngines		x
Total	1	2



Management - SportsGoodsCMA

Report for revisions 16 on SportsGoodsCMA and 26 on HamburgCMA

Recent revision

Revision	Action	Date	Time	Date on Device	Time on Device	Administrator	Installed On	GUI Client	Audit Log	Global Policy	Ticket ID
16	Save Policy	11 Nov 2007	01:15:59	10 Nov 2007	17:48:15	John		Nova	455	-	

Аудит

Сокращает время аудита до нескольких часов

Предлагает решения в случае нарушений

Может быть использован аудитором или сотрудниками

Поддержка PCI DSS 2.0 по умолчанию



Автоматическая проверка соответствия по многим параметрам относящимся к сетевой безопасности

DCR

Специально разработан для маршрутизаторов и коммутаторов Cisco

Соответствует CIS и NSA Router Security Configuration Guide

Проверка основных настроек безопасности, внесение рекомендуемых изменений в конфигурацию

Tufin Device Audit - 'Tufin Device Audit 11/07/2011'

Generated on Thu, 14 Jul 2011, 11:00:27 by admin
Report Time: Thu, 14 Jul 2011, 11:00

Cisco Router - Cisco Router 2801
Policy Package: Standard

Revision:

Revision	Action	Date	Time	Date on Device	Time on Device	Administrator	Installed On	GUI Client	Audit Log	Policy Package	Global Policy	Ticket ID
4	Automatic	Wed, 06 Jul 2011	13:49:08	Wed, 06 Jul 2011	13:49:07	-	-	-	-	Standard	-	-

Tests summary:

#	UID	Name	Severity	Status	Details
1	TF001	Require AAA Service	High	Failed	Details
2	TF002	Require AAA Authentication for Login	High	Failed	Details
3	TF003	Require AAA Authentication for Enable Mode	High	Failed	Details
4	TF004	Require AAA Authentication for Local Aux Lines	High	Failed	Details
5	TF005	Require AAA Authentication for Local Console Lines	High	Failed	Details
6	TF006	Require AAA Authentication for Local TTY Lines	High	Failed	Details
7	TF007	Require AAA Authentication for Local VTY Lines	High	Failed	Details
8	TF008	Require Privilege Level 1 for Local Users	High	Passed	Details
9	TF009	Require SSH Server Version 2	High	Passed	Details
10	TF010	Require SSH Server Timeout	High	Failed	Details
11	TF011	Require SSH Server Authentication Retries Max	High	Failed	Details
12	TF012	Require VTY Transport SSH	High	Failed	Details
13	TF013	Require Timeout for Login Sessions on Aux Lines	High	Passed	Details
14	TF014	Require Timeout for Login Sessions on Console Lines	High	Failed	Details
15	TF015	Require Timeout for Login Sessions on TTY Lines	High	Failed	Details
16	TF016	Require Timeout for Login Sessions on VTY Lines	High	Failed	Details
17	TF017	Forbid Auxiliary Port	High	Failed	Details
18	TF018	Require SSH Access Control	High	Passed	Details
19	TF019	Require VTY ACL	High	Failed	Details
20	TF020	Require EXEC Banner	High	Failed	Details
21	TF020	Require Login Banner	High	Failed	Details
22	TF022	Require MOTD Banner	High	Failed	Details
23	TF023	Require Enable Secret	High	Failed	Details
24	TF024	Require Password Encryption Service	High	Passed	Details

(admin) Global
Licensed to Customer 1 Attention Required

SNMP

NTP

Syslog

Аутентификация

Ненужные
сервисы

**tufin**

        	Финансовая отрасль
            	Телеком
      	Транспорт
     	Энергетика
            	Здравоохранение
        	Другие



- отдельно лицензируются кластеры устройств

- к каждой лицензируемой позиции добавляется поддержка от вендора



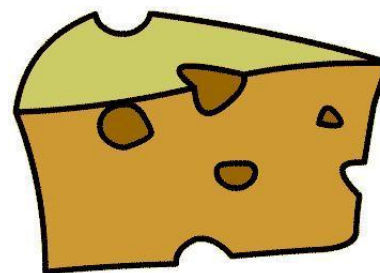
Можно
запросить
полноценную
триальную
версию на 30
дней

Дистрибуция
продукта
открытая,
проводится
обучение в
России

tufin

Высокое
качество
работы сервиса
поддержки от
вендора

Возможна
покупка
программно-
аппаратного
комплекса



Имеется
возможность
поддержки от
вендора на
русском языке

www.tufin.com
www.rrc.ru

Спасибо за внимание!

pkuzeev@rrc.ru
Skype – **zerottl**
+7 985 9994824