

Tufin Security Suite

nástroje pro audit, archivaci a podporu správy bezpečnostních politik



Martin Slavík
msl@actinet.cz



představení



- kdo je Tufin?
- proč jsme vybrali právě Tufin?
- kam vyrostli?

představení



výzvy bezpečnosti IT



- komplexita prostředí 
 - orientace, chaos, náchylnost k chybám, nestabilita
- shoda se standardy 
 - korporátními politikami, normami (SOX, PCI)
- procesy 
 - životní cyklus bezpečnosti, metodiky (firemní, ITIL), auditní procesy

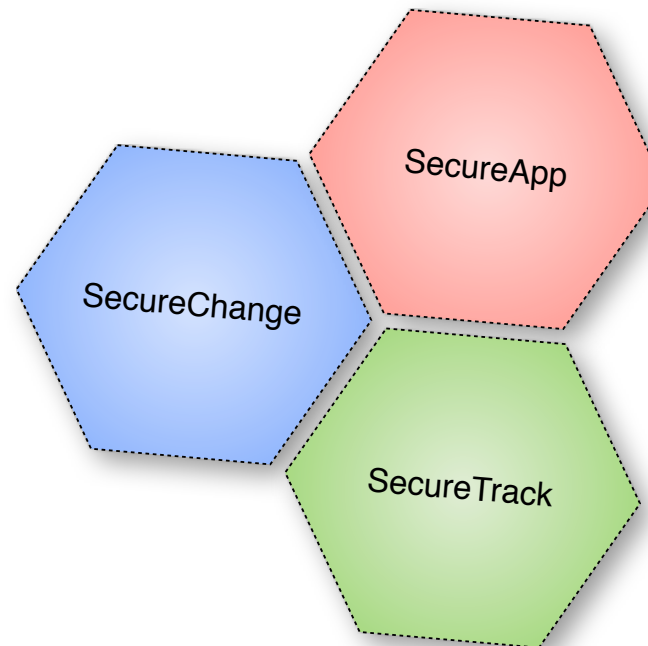


máte vhodný nástroj?

Tufin Security Suite



- SecureTrack
 - vstup dat, analýza, compliance
- SecureChange
 - změnové řízení, workflow
- SecureApp
 - tvorba fw politiky ,done right‘



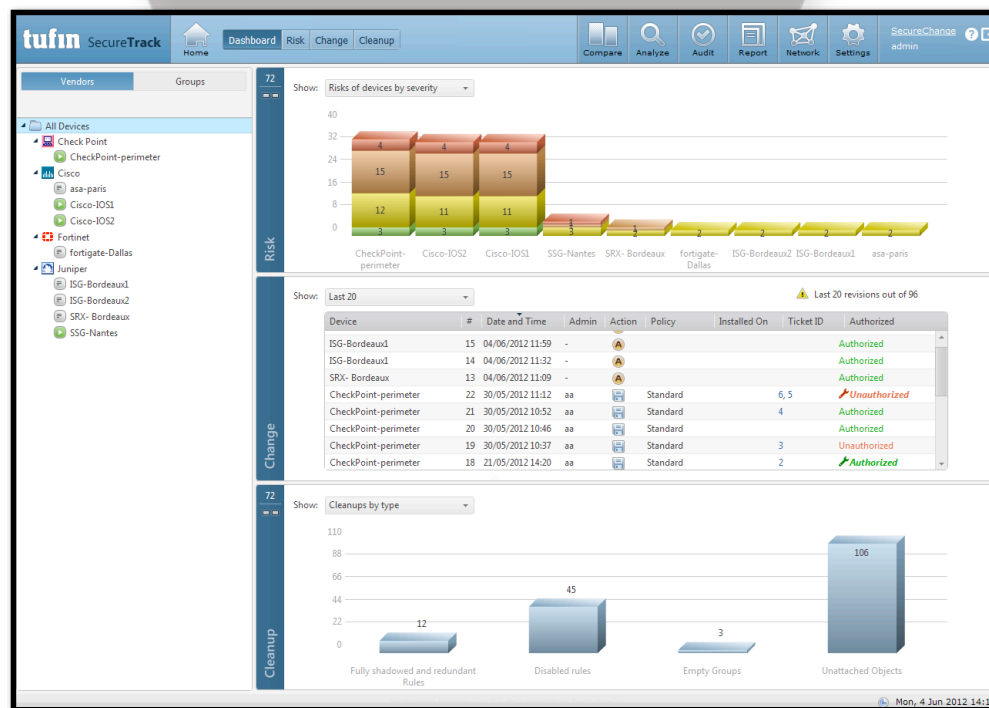
SecureTrack

tufin
Making Security Manageable

• vstup dat

• reporty

• analýzy



SecureTrack

tufin
Making Security Manageable

- vstup dat

- reporty

- analýzy

Revision History - CheckPoint-perimeter - 22 revisions during the last year

Revision	Action	Date	Time	Administrator	Installed on	GUI client	Audit log	Policy package	Global policy	Ticket ID	Comment
22		Wed, 30 May 2012	11:12:33	aa	-	Amir-Laptop	4987	Standard	-	5,6	Click to edit...
21		Wed, 30 May 2012	10:52:56	aa	-	Amir-Laptop	4984	Standard	-	4	Click to edit...
20		Wed, 30 May 2012	10:46:21	aa	-	Amir-Laptop	4981	Standard	-	-	Click to edit...

Filter View Policy Compare Generate Report

Comparison

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

Security Address Translation

Standard

CheckPoint-perimeter - Revision 21 - aa - Wed, 30 May 2012 10:52:56

NO.	NAME	SOURCE	DESTINATION	VPN SERVICE	ACTION	TRACK	INSTALL ON	TIME	COM
Customer access in									
1	customer1Net	billManager	financePortal	Any	accept	None	Any	Any	
2	customer1Net	h_105	h_177	Any	accept	None	Any	Any	
3	customer1Net	customer2Net	ftpServer	Any	http	accept	None	Any	
DMZ outbound									
Local network outbound									
4	Any	gateway_external	cpmodule	Any	accept	None	Any	Any	
5	Any	gateway_external	cpmodule	Any	accept	None	Any	Any	
6	Any	Any	Any	Any	drop	Log	Any	Any	

Standard

CheckPoint-perimeter - Revision 22 - aa - Wed, 30 May 2012 11:12:33

NO.	NAME	SOURCE	DESTINATION	VPN SERVICE	ACTION	TRACK	INSTALL ON	TIME	COM
Customer access in									
1	customer1Net	billManager	financePortal	Any	accept	None	Any	Any	
2	customer1Net	h_105	h_177	Any	accept	None	Any	Any	
3	customer1Net	customer2Net	ftpServer	Any	http	accept	None	Any	
4	customer3Net	LotusSrvr	Any	Any	http	accept	None	Any	
DMZ outbound									
Local network outbound									
5	Any	gateway_external	cpmodule	Any	accept	None	Any	Any	
6	Any	gateway_external	cpmodule	Any	accept	None	Any	Any	
7	Any	Any	Any	Any	drop	Log	Any	Any	

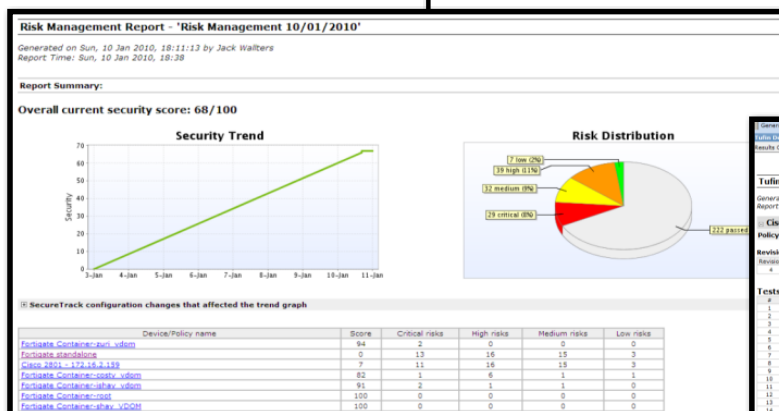
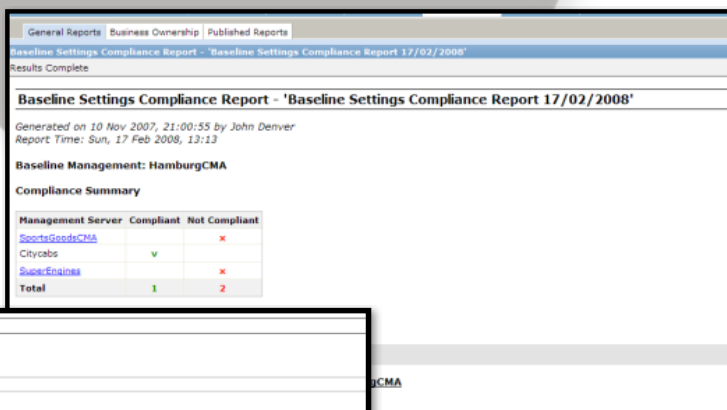
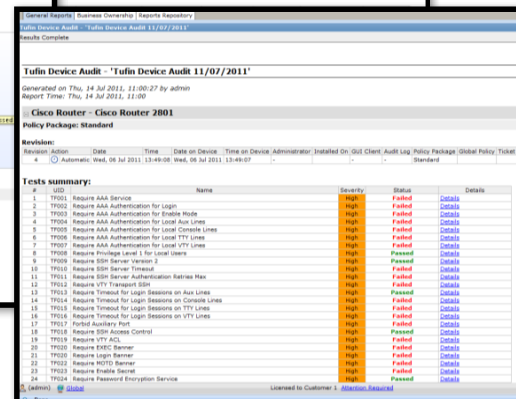
SecureTrack

tufin
Making Security Manageable

• vstup dat

• analýzy

• reporty

Revision	Author	Date	Time	Device	Time on Device	Administrator	Installed On	Used Client	Audit Log	Policy Package	Global Policy	Ticket ID
1	Automatic	Wed, 08 Jul 2011	13:49:08	Wed, 08 Jul 2011	13:49:07					Standard		

Tests summary:

#	UD	Name	Severity	Status	Details
1	UD01	Require AAA Service	High	Failed	Details
2	UD02	Require AAA Authentication for Login	High	Failed	Details
3	UD03	Require AAA Authentication for Shell Users	High	Failed	Details
4	UD04	Require AAA Authentication for Local Aux Lines	High	Failed	Details
5	UD05	Require AAA Authentication for Local Console Lines	High	Failed	Details
6	UD06	Require AAA Authentication for Local VTY Lines	High	Failed	Details
7	UD07	Require AAA Authentication for Local VTY Lines	High	Failed	Details
8	UD08	Require Privilege Level 1 for Local Users	High	Passed	Details
9	UD09	Require SSH Server Version 3	High	Passed	Details
10	UD10	Require SSH Server Timeout	High	Failed	Details
11	UD11	Require SSH Server Authentication Radius Max	High	Failed	Details
12	UD12	Require VTY Transport SSH	High	Failed	Details
13	UD13	Require Timeout for Login Sessions on Aux Lines	High	Failed	Details
14	UD14	Require Timeout for Login Sessions on Console Lines	High	Failed	Details
15	UD15	Require Timeout for Login Sessions on VTY Lines	High	Failed	Details
16	UD16	Require Timeout for Login Sessions on VTY Lines	High	Failed	Details
17	UD17	Require Auxiliary Port	High	Failed	Details
18	UD18	Require SSH Access Control	High	Passed	Details
19	UD19	Require VTY ACL	High	Failed	Details
20	UD20	Require EXEC Banner	High	Failed	Details
21	UD21	Require Login Banner	High	Failed	Details
22	UD22	Require MOTD Banner	High	Failed	Details
23	UD23	Require Enable Secret	High	Failed	Details
24	UD24	Require Password Encryption Service	High	Passed	Details

SecureChange

- změnové řízení
- automatizace

- podpora standardů
- vaše workflow



SecureChange

- změnové řízení
- automatizace

- podpora standardů
- vaše workflow

tufin
Making Security Manageable

1

2

3

Step name: Security Review and approval

Required Access ⓘ

Risk Analysis Import

Target	Source
SMC_192.168.3.15/Sample1	192.168.5.57 192.168.5.56

RSK

DSR

ADV

VER

AR1

tufin

SecureChange

Tasks My Requests Reports Workflows Dashboard

Settings Maya

MY TICKETS

SLA	ID	Subject	Step	Duration	Assigned to	Requestor	Workflow
N/A	6	Need access to TSS	Technical Design	1 Day	Maya	Alan	Sample Access Request
N/A	5	Need access to Lotus Notes	Technical Design	1 Day	Maya	Alan	Sample Access Request
N/A	4	Asking for internet access	Generic Request Approval	1 Day	Maya	Robert	Sample Generic Request
N/A	2	Need access to Exchange	Implementation	1 Day	Maya	Maya	Sample Access Request
N/A	1	Need access to CRM	Technical Design	1 Day	Maya	Maya	Sample Access Request

#6 | NEED ACCESS TO TSS

Request is required until: None priority: Normal

Step name: Technical Design Handler: Maya

Required Access ⓘ

Risk Analysis Designer Import

Target	Source	Destination	Service	Action	Comment
ANY	192.168.1.115	10.100.101.63	https	Accept	

Design comment ⓘ

Save Done

SecureChange

tufin
Making Security Manageable

- změnové řízení
- automatizace

- podpora standardů
- vaše workflow

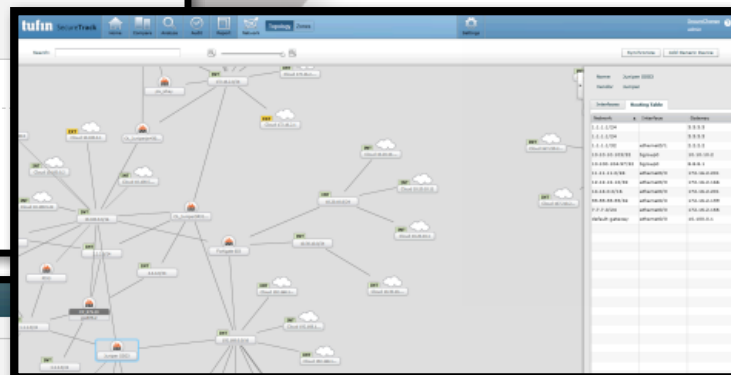
Designer

The following changes are recommended for your access requests:

• **SMC_192.168.3.15/Sample1**

AR1 (for SMC_192.168.3.15/Sample1)

- Add new network object Host_192.168.5.56: 192.168.5.56
- Rule.2: Add source Host_192.168.5.56, Host_192.168.5.57



Verification

SMC_192.168.3.15, Installed on modules: cpmodule

Revision number: 22 Date: 2012-07-02 Time: 15:05:15 Administrator: Maya_3_11

Status: **Verified**

Implementing rules

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
2		Host_1.1.1.1 Host_1.1.1.4 Host_192.168.5.56 Host_192.168.5.57	Host_192.168.3.100	* Any	TCP telnet	accept	None	* Any	* Any	

No violating rules

SecureApp

- katalog aplikací
- komunikační mapy

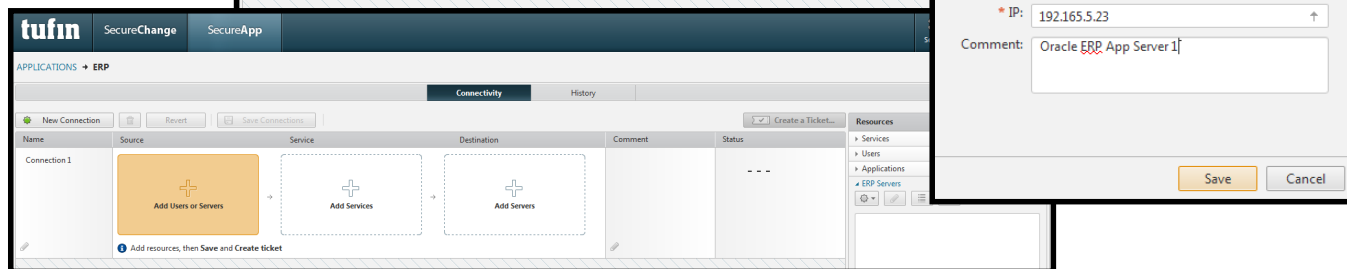
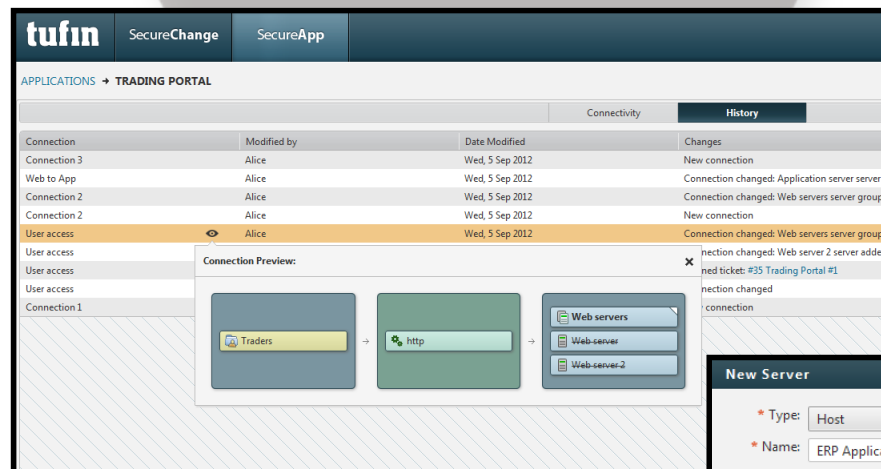
- workflow vazby



SecureApp

- katalog aplikací
- komunikační mapy

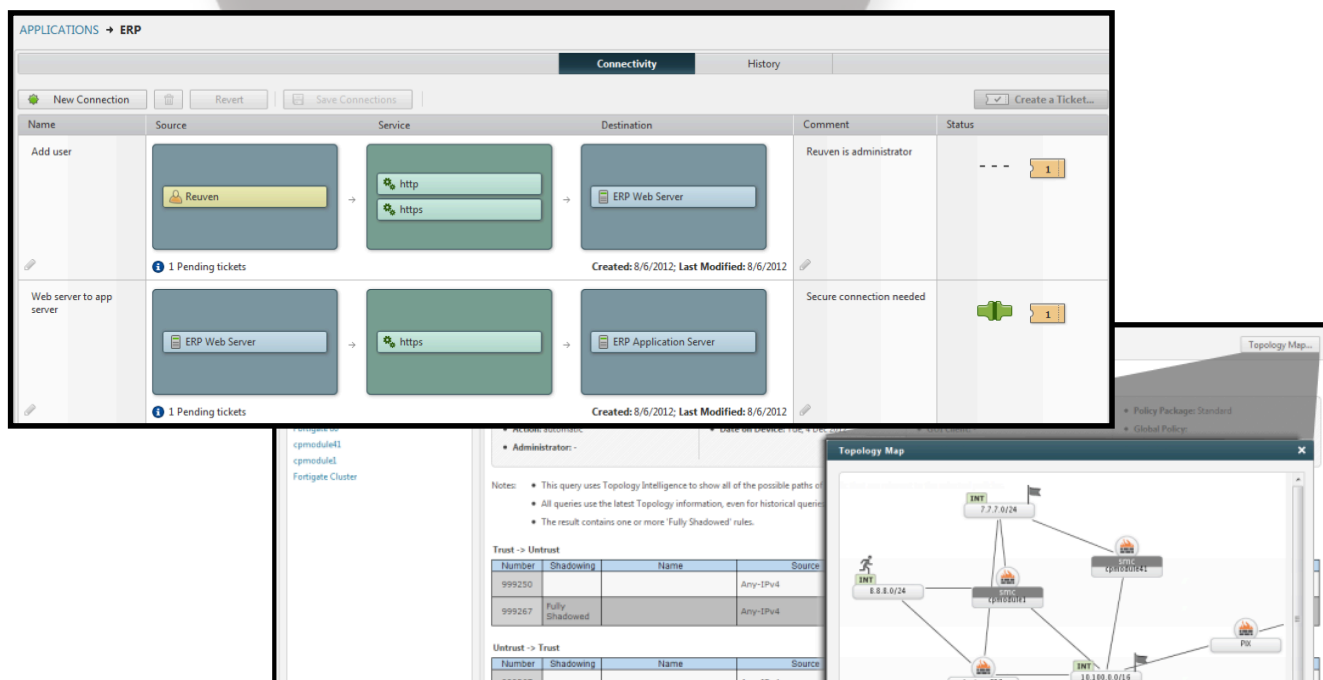
- workflow vazby



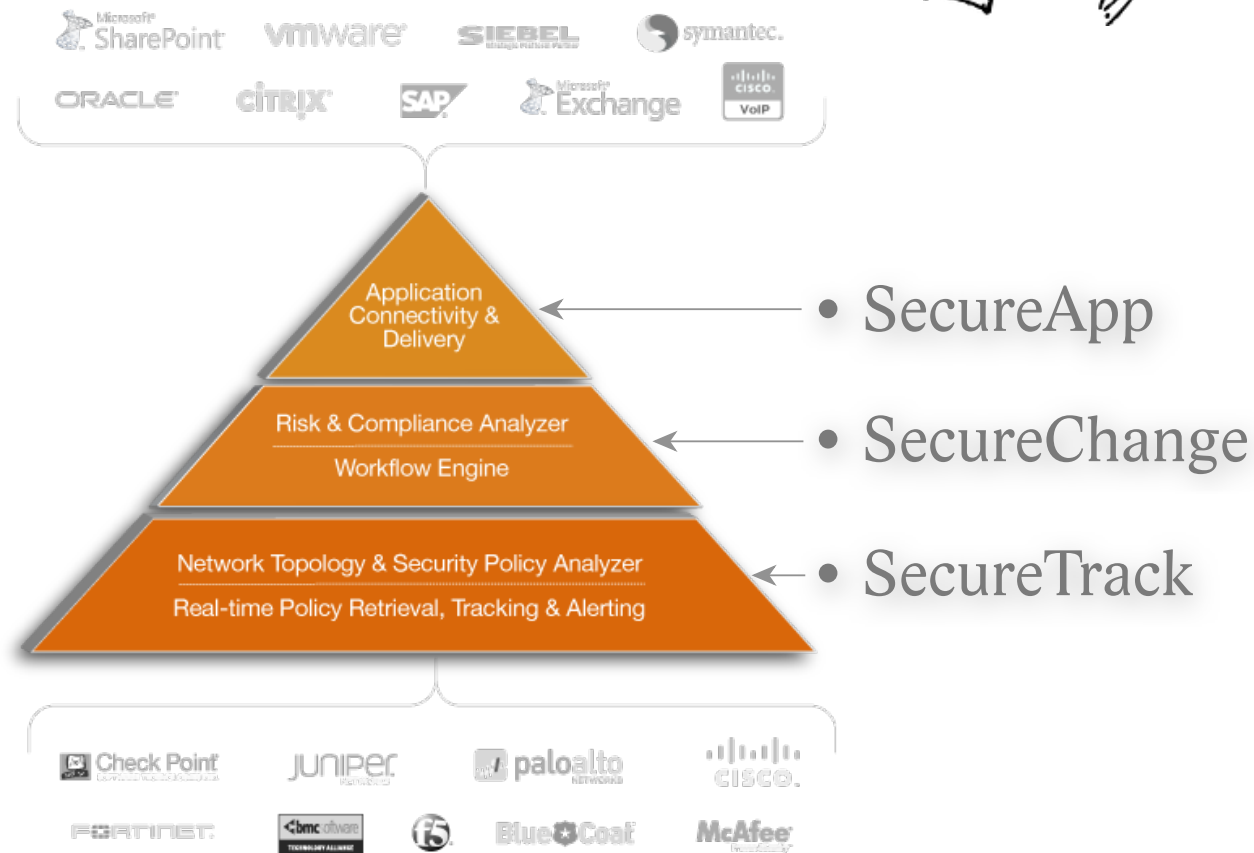
SecureApp

- katalog aplikací
- komunikační mapy

- workflow vazby



Tufin – The Big Picture



děkuji za pozornost



Martin Slavík
msl@actinet.cz

