

# 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

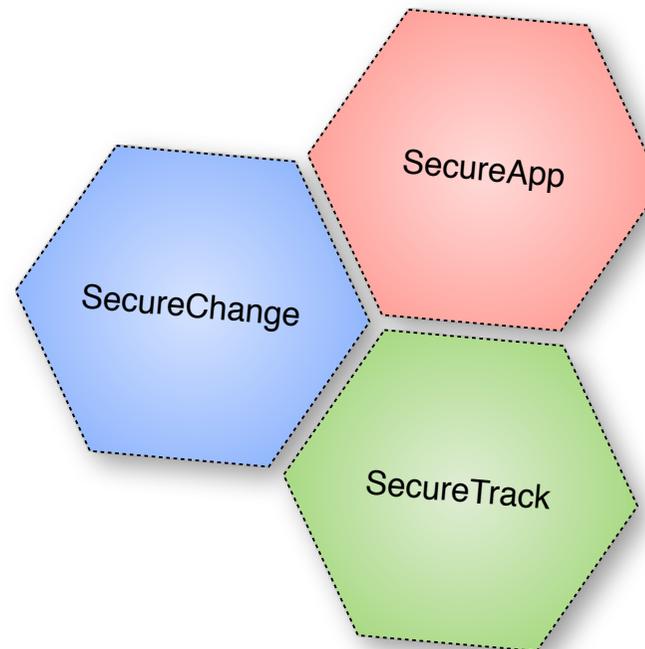


máte vhodný nástroj?

# Tufin Security Suite



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



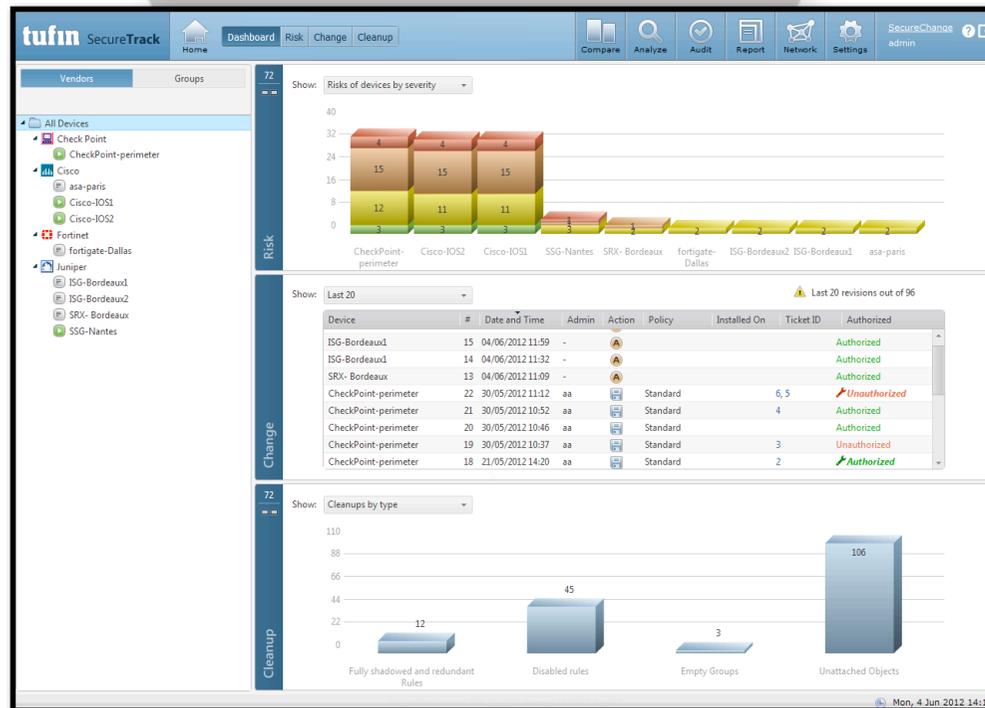
# SecureTrack

tufin  
Making Security Manageable

- vstup dat

- reporty

- analýzy



# SecureTrack



- 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	<a href="#">Click to edit...</a>
21		Wed, 30 May 2012	10:52:56	aa	-	Amir-Laptop	4984	Standard	-	4	<a href="#">Click to edit...</a>
20		Wed, 30 May 2012	10:46:21	aa	-	Amir-Laptop	4981	Standard	-		<a href="#">Click to edit...</a>

Filter View Policy Compare Generate Report

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

Security Address Translation

Standard 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	Any	accept	-	Any	Any
2		customer1Net	h_105 h_177	Any	Any	accept	-	Any	Any
3		customer1Net customer2Net	ftpServer	Any	http	accept	-	Any	Any
DMZ outbound									
Local network outbound									
4		Any	gateway_external cpmodule	Any	Any	accept	-	Any	Any
5		Any	gateway_external cpmodule	Any	Any	accept	-	Any	Any
6		Any	Any	Any	Any	drop	Log	Any	Any

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	Any	accept	-	Any	Any
2		customer1Net	h_105 h_177	Any	Any	accept	-	Any	Any
3		customer1Net customer2Net customer3Net	ftpServer	Any	http	accept	-	Any	Any
4		customer3Net	LotusSrvr	Any	http	accept	-	Any	Any
DMZ outbound									
Local network outbound									
5		Any	gateway_external cpmodule	Any	Any	accept	-	Any	Any
6		Any	gateway_external cpmodule	Any	Any	accept	-	Any	Any
7		Any	Any	Any	Any	drop	Log	Any	Any

# SecureTrack



- vstup dat

- reporty

- analýzy

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
SportsGondCMA		x
Citycabs	v	
SuperEngines		x
<b>Total</b>	<b>1</b>	<b>2</b>

**Risk Management Report - 'Risk Management 10/01/2010'**

Generated on Sun, 10 Jan 2010, 18:11:13 by Jack Walters  
Report Time: Sun, 10 Jan 2010, 18:38

Report Summary:

Overall current security score: 68/100

**Security Trend**

**Risk Distribution**

SecureTrack configuration changes that affected the trend graph

Device/Policy name	Score	Critical risks	High risks	Medium risks	Low risks
Foxtaste_Centrac-fact_vdcm	94	2	0	0	0
Foxtaste_mediacore	0	13	16	15	3
Cisco-2801-172.16.2.132	7	11	16	15	3
Foxtaste_Centrac-coast_vdcm	82	1	6	1	1
Foxtaste_Centrac-cultra_vdcm	91	2	1	1	0
Foxtaste_Centrac-coast	100	0	0	0	0
Foxtaste_Centrac-play_VDCC	100	0	0	0	0

General Reports | Business Ownership | Reports Repository

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

Results Complete

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

**Cisco Router - Cisco Router 2801**

Policy Package: Standard

Revisions:

Revision	Author	Date	Time	Done on Device	Done on Administrator	Installed On	Used Client	Audit Log	Policy Package	Global Policy	Ticket ID
4	Automatic	Wed, 08 Jul 2011	13:49:08	Used	Used	08 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 Shell Privs	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 VTY 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 3	High	Passed	Details
10	TF010	Require SSH Server Timeout	High	Failed	Details
11	TF011	Require SSH Server Authentication Failure Max	High	Failed	Details
12	TF012	Require VTY Transport SSH	High	Failed	Details
13	TF013	Require Timeout for Login Sessions on Aux Lines	High	Failed	Details
14	TF014	Require Timeout for Login Sessions on Console Lines	High	Failed	Details
15	TF015	Require Timeout for Login Sessions on VTY Lines	High	Failed	Details
16	TF016	Require Timeout for Login Sessions on VTY Lines	High	Failed	Details
17	TF017	Require 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	TF021	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

# SecureChange

- změnové řízení
- automatizace

- podpora standardů
- vaše workflow



# SecureChange

- změnové řízení
- automatizace

- podpora standardů
- vaše workflow



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



- změnové řízení
- automatizace

- podpora standardů
- vaše workflow

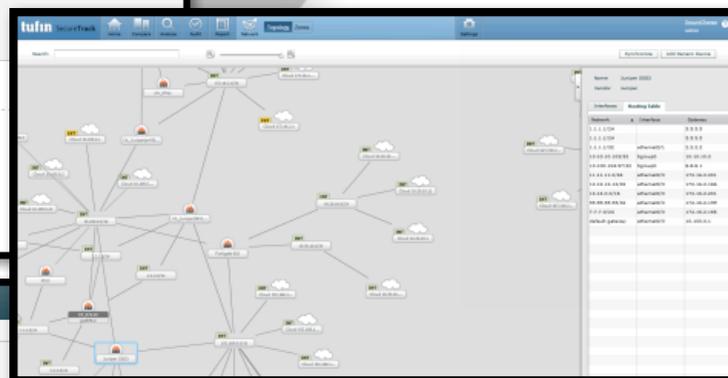
**Designer**

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		<ul style="list-style-type: none"> <li>Host_1.1.1.1</li> <li>Host_1.1.1.4</li> <li>Host_192.168.5.56</li> <li>Host_192.168.5.57</li> </ul>	Host_192.168.3.100	* Any	TCP telnet	accept	- None	* Any	* Any	

No violating rules

# SecureApp



- katalog aplikací
- komunikační mapy

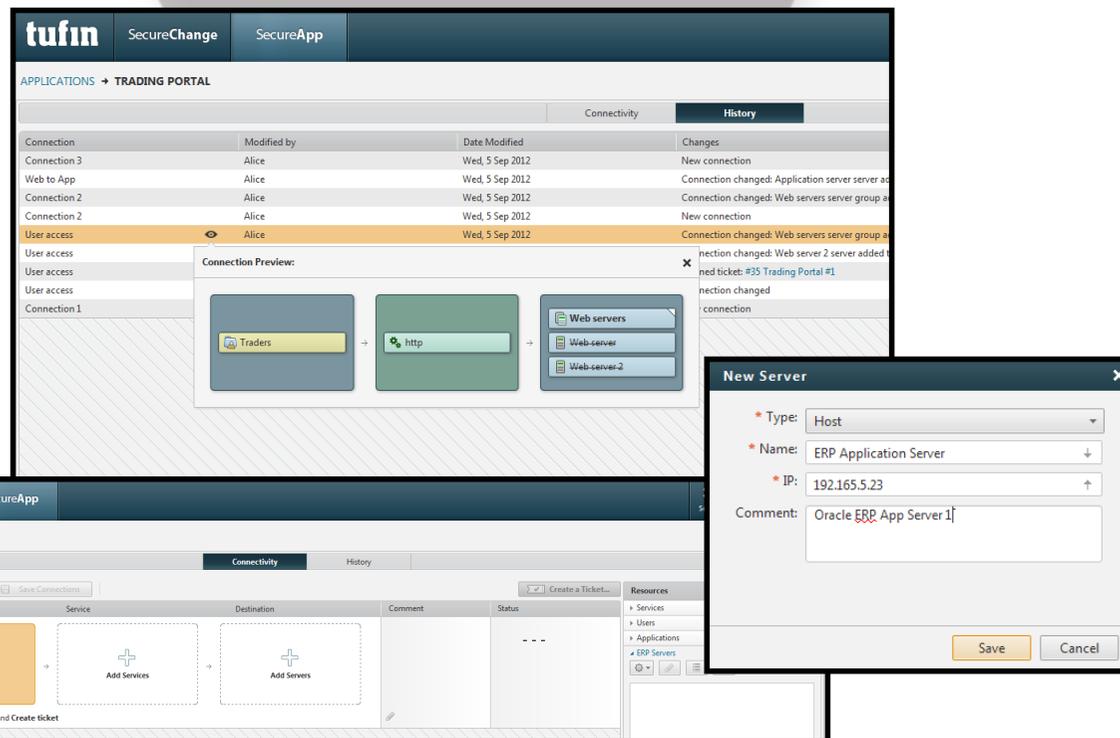
- workflow vazby



# SecureApp

- katalog aplikací
- komunikační mapy

- workflow vazby



The image displays two screenshots of the tufin SecureApp interface. The top screenshot shows the 'APPLICATIONS → TRADING PORTAL' view with a table of connections and a 'Connection Preview' window. The bottom screenshot shows the 'APPLICATIONS → ERP' view with a 'New Server' dialog box open.

Connection	Modified by	Date Modified	Changes
Connection 3	Alice	Wed, 5 Sep 2012	New connection
Web to App	Alice	Wed, 5 Sep 2012	Connection changed: Application server server as
Connection 2	Alice	Wed, 5 Sep 2012	Connection changed: Web servers server group a
Connection 2	Alice	Wed, 5 Sep 2012	New connection
User access	Alice	Wed, 5 Sep 2012	Connection changed: Web servers server group a
User access			Connection changed: Web server 2 server added t
User access			Connection changed: #35 Trading Portal #1
User access			Connection changed
Connection 1			Connection changed

**Connection Preview:**

Traders → http → Web servers (Web-server, Web-server-2)

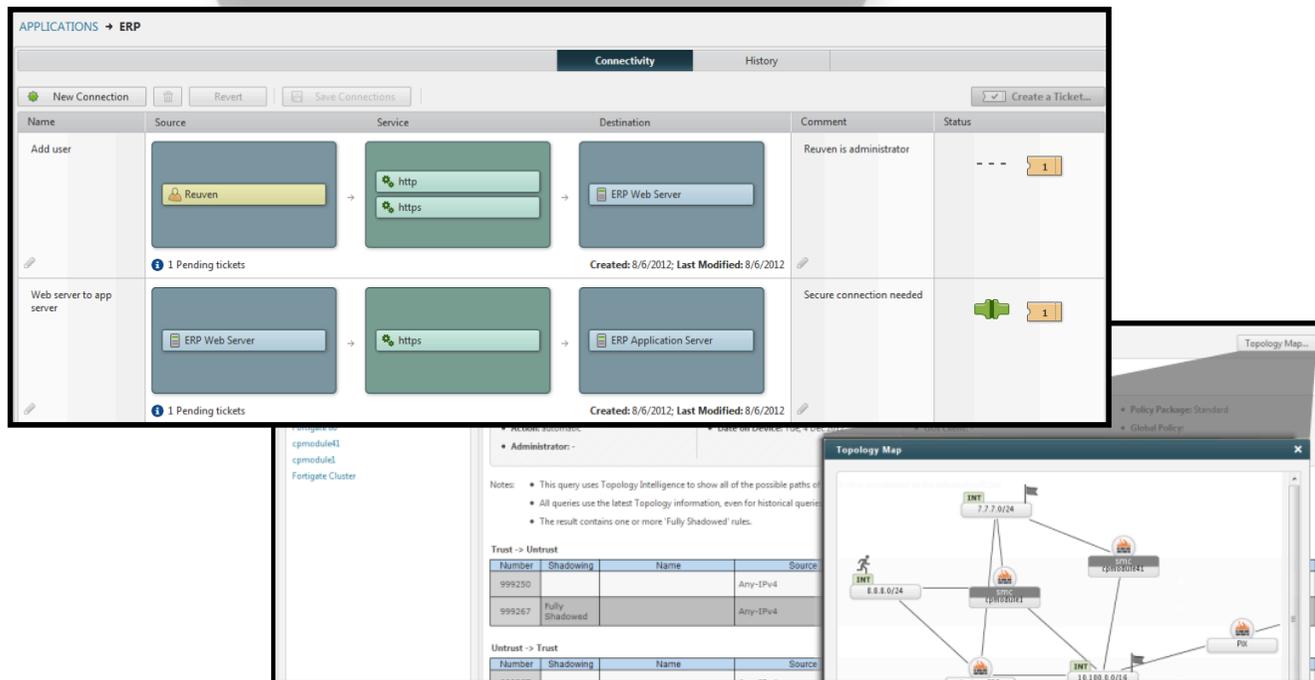
**New Server Dialog:**

- Type: Host
- Name: ERP Application Server
- IP: 192.165.5.23
- Comment: Oracle ERP App Server 1

# SecureApp

- katalog aplikací
- komunikační mapy

- workflow vazby



The screenshot displays the SecureApp interface, which is used for managing application connectivity and security. The main window shows a list of connections under the 'Connectivity' tab. Two connections are visible:

- Add user:** Source: Reuven; Service: http, https; Destination: ERP Web Server. Comment: Reuven is administrator. Status: 1 Pending tickets.
- Web server to app server:** Source: ERP Web Server; Service: https; Destination: ERP Application Server. Comment: Secure connection needed. Status: 1 Pending tickets.

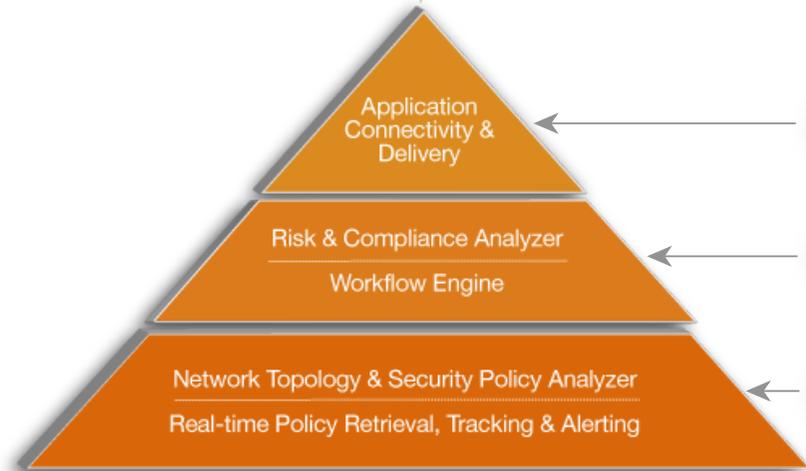
Below the connectivity list, there are two overlapping windows:

- Topology Map:** A network diagram showing various nodes and their connections. Nodes include 'SNT 7.7.0/24', 'SNT 8.0.0/24', 'SNT 8.100.0/16', and 'Pix'. The diagram illustrates the network topology and how it relates to the application connectivity.
- Trust/Untrust Table:** A table showing the results of a query for trust and untrust relationships. The table has columns for Number, Shadowing, Name, and Source.

Trust -> Untrust			
Number	Shadowing	Name	Source
999250			Any-IPv4
999267	Fully Shadowed		Any-IPv4

Untrust -> Trust			
Number	Shadowing	Name	Source

# Tufin – The Big Picture



- SecureApp
- SecureChange
- SecureTrack



**děkuji za pozornost**



Martin Slavík  
msl@actinet.cz

