

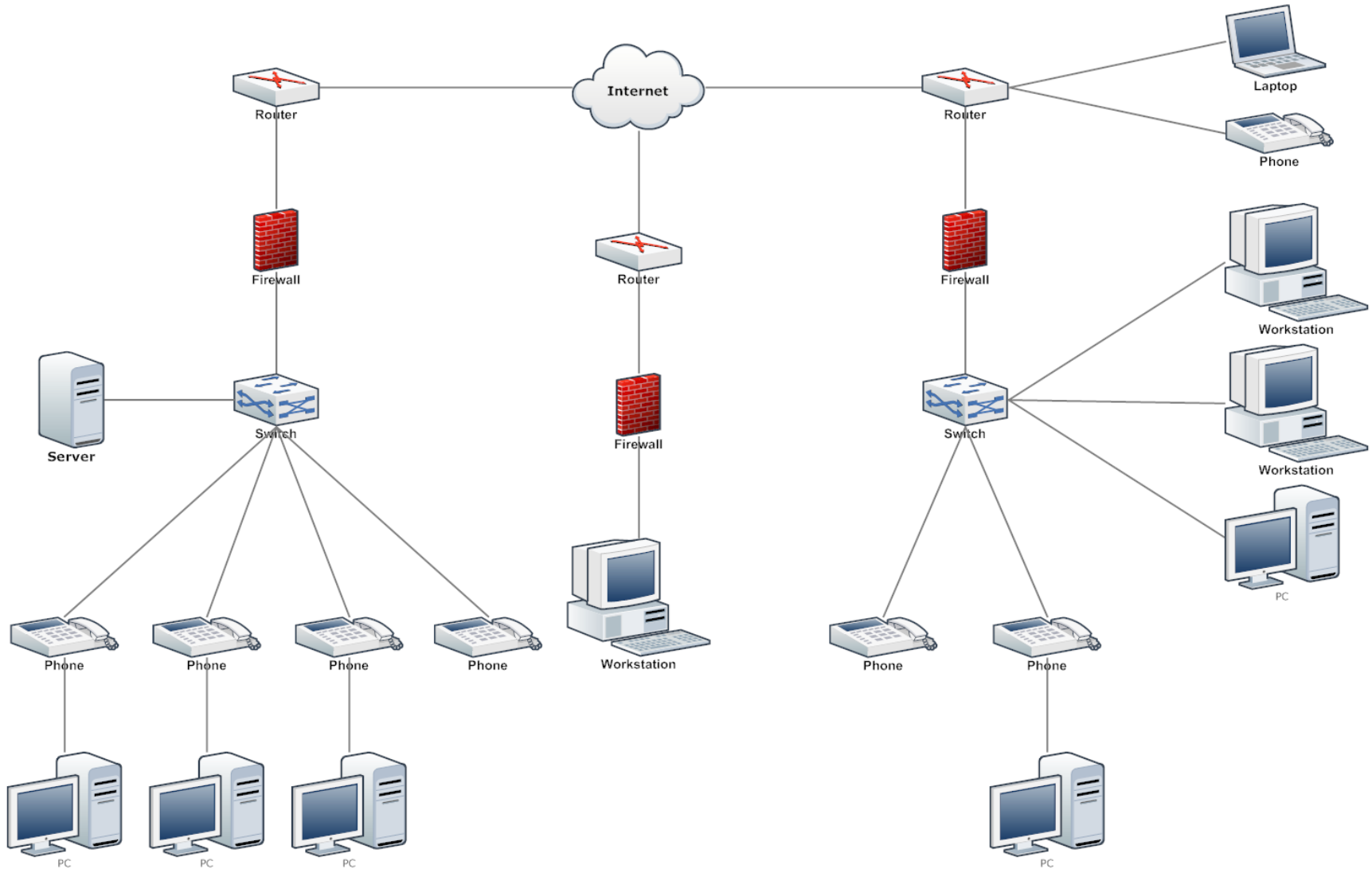


2020

Фаєрволи. Просте управління  
складними рішеннями

Денис Фомкін  
[nwu.com.ua](http://nwu.com.ua)

# Firewall

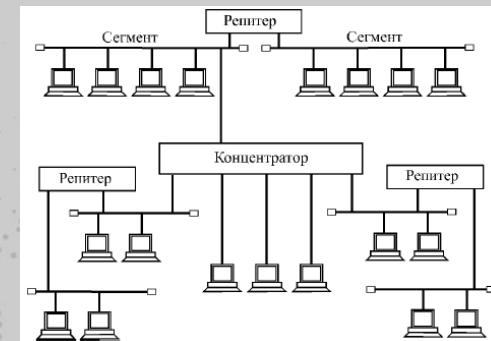


Є політика захисту доступу по мережі - але немає контролю управління змінами. Чому?

1. Обладнання не змінюють роками - правила доступу каскадні (100>)
2. Там купили Palo Alto а там - Cisco, а тут ще є Fortinet
3. Жодна консоль не покаже «А що якщо я так зроблю?»
4. Ні в одну консоль НЕ занесеш правила ІБ
5. «А хто в цьому винен?» - коли щось трапляється (ІТ та ІБ)



- ✓ **Засіб організації і підтримки порядку в ACL:**
  - Дублюючі, затінюючі, невикористовувані об'єкти і правила
  - Фактичне використання правил - оптимізація
- ✓ **Єдина точка аналізу і просування правил доступу:**
  - Єдина консоль на Cisco, Checkpoint, Juniper, F5 і ін.
  - Контроль логічного доступу в регіонах
  - Підтримка застарілого обладнання і нестабільних каналів
- ✓ **Оперативний аналіз доступів будь-якої складності:**
  - Вплив NAT-правил, врахування динамічної та статичної маршрутизації
  - Підтримка віртуальних систем і ПАК (VMware + OpenStack)



✓ **Засіб оцінки прийнятності доступу:**

- Бази загальних ризиків («типових помилок»);
- Внесення в систему політик ІБ у вигляді простих правил МЕ

✓ **Фіксація і формалізація дій щодо доступу:**

- Розподіл відповідальності за етапами обробки (шаблони);
- Пряма прив'язка до технічного рівня, до мережі
- Ресертифікація правил

✓ **Оперативна інформація про зміни в доступі:**

- У реальному часі за фактом зміни, по всій структурі;
- База подій за минулий час по всій структурі

✓ **Підтримка відповідності міжнародних стандартів:**

- PCI DSS, SOX, GDPR;





SecureTrack

- ✓ Автоматизований контроль і аналіз мережевого доступу
- ✓ На рівні мережного обладнання від різних вендорів
- ✓ ІТ- підрозділи, мережеві фахівці, сисадміни

Функціонал, що не надається консолями ЦК окремих виробників



SecureChange

- ✓ Формування та обробка додатків для доступу в Інтернет
- ✓ Дизайн, аналіз ризиків і безпеки
- ✓ ІБ підрозділи, а не технічний персонал

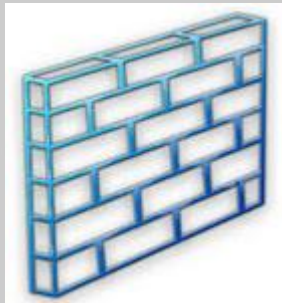
Процеси доступу до бізнесу, Автоматизація впровадження, оцінка безпеки



SecureApp

- ✓ Контроль за доступністю додатків 24X7
- ✓ Блокування порушень зв'язку між і з додатками
- ✓ Відділи розробки, обслуговування платіжних систем

Модуль захисту доступу для критичних додатків



Start monitoring a new device:

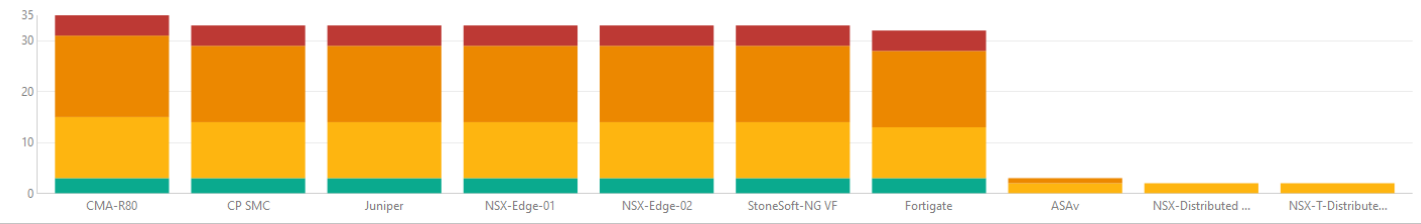
 Select Device	 Select Device	 Select Device	 Select Device	 Select Device
 Select Device	 Select Device	 Select Device	 Select Device	 Select Device
 Select Device	 Select Device	 Select Device		

- ✓ Підтримка керуючих консолей та окремих пристроїв від провідних постачальників: Juniper, Palo Alto (PA – Services/Users), Cisco, Fortinet, McAfee, Stonesoft, BlueCoat, F5 BIG IP та інші...
- ✓ Все, що Linux/Unix на основі IPTables
- ✓ Комутатори, NLB, Generic Type, хмарні ресурси

- Vendors** | Groups
- All Devices
    - 1Toronto BCKP
      - Check Point
        - Provider-1 MDS
          - CMA-R80
      - Cisco
        - Cisco Firepower
          - Domain\_1
            - Domain\_1\_1
            - Domain\_2
          - Domain\_2
            - Domain\_2\_1
            - Domain\_2\_2
      - Fortinet
        - Fortigate
      - Amsterdam
        - Cisco
          - RTR6
        - Fortinet
          - FortiManager-Advanced Mode
            - Amsterdam
      - Default
        - Cisco
          - ACI Fabric
            - ACI Fabric-Design-Team
            - ACI Fabric-Topology-Team
          - Pe\_1
          - Pe\_2
          - RTR1
          - RTR2
        - Juniper
          - Juniper
            - SRX
        - HQ - California
          - Cisco
            - ASA
          - Palo Alto Networks
            - ...

**Risk** 72

Show: Risks of devices by severity



**Change**

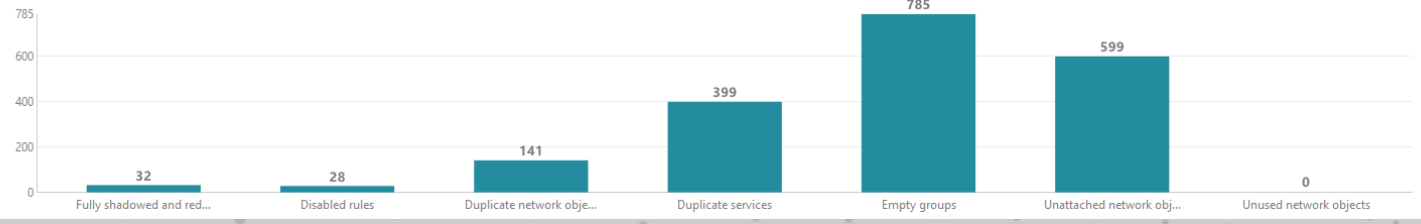
Show: Last 20

Last 20 revisions out of 1,805

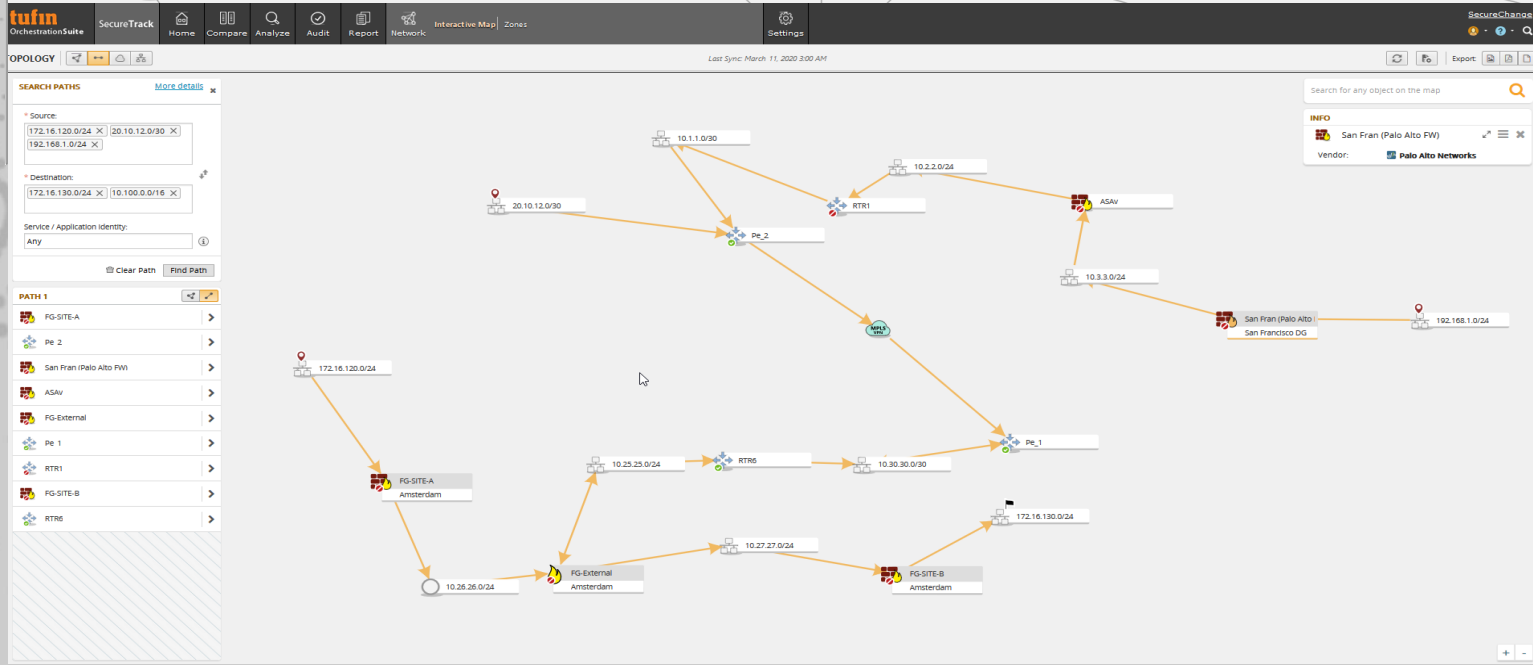
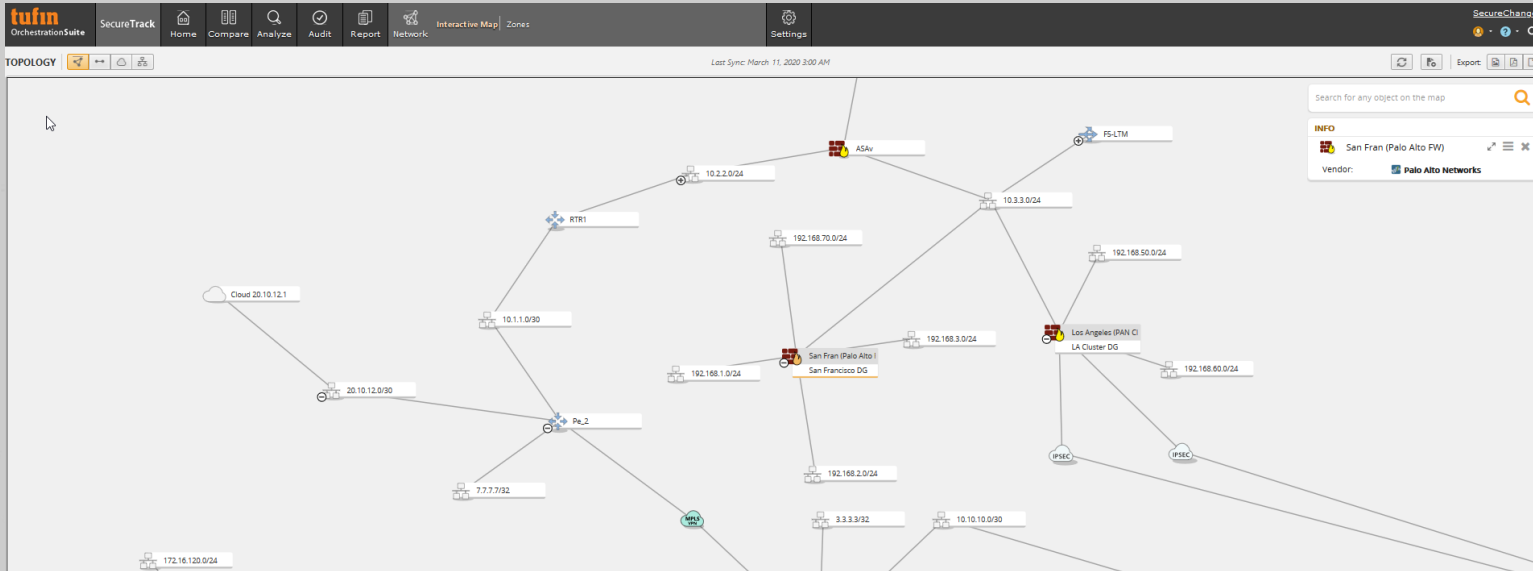
Device	#	Changed on	Received on	Admin	Action	Policy	Installed On	Ticket ID	Authorized
Juniper	1	2/26/20 6:42 PM	2/26/20 6:42 PM	root	A				N/A
San Francisco DG	250	12/24/19 10:42 AM	12/24/19 10:46 AM		A			138, 147, 20	Unauthorized
LA Cluster DG	189	12/24/19 10:42 AM	12/24/19 10:45 AM		A				Authorized
Panorama-DG	132	12/24/19 10:42 AM	12/24/19 10:45 AM		A				Unauthorized
Amsterdam	53	12/22/19 7:10 PM	12/22/19 7:11 PM	-	A				Authorized
Amsterdam	52	12/19/19 3:26 PM	12/19/19 3:26 PM		A			241	Unauthorized
Amsterdam	51	12/19/19 3:16 PM	12/19/19 3:16 PM		A				Authorized

**Cleanup** 92

Show: Cleanups by type







Required Access ⓘ

Risk Analysis | Designer | Verifier | Import

	Target	Source	Destination	Service/Application Identity	Action	Comment
☰	CP SMC/SMCPM	172.16.40.0/24	10.11.11.0/30	smtp	Accept	
+	RTR4					

- ✓ RSK
- DSR
- VER
- AR1

**Designer**

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

**CHECK POINT** Update All Policies

**CP SMC** Update Policy

→ Standard

**AR1** (For CP SMC/Standard) ⓘ

- Add new network object [Subnet 172.16.40.0](#)
- Add new network object [Host 172.16.40.100\\_1](#)
- Add new network object [Subnet 10.11.11.0](#)
- Add new rule <Name> before rule: 37 [View Rule](#) [View Policy](#)

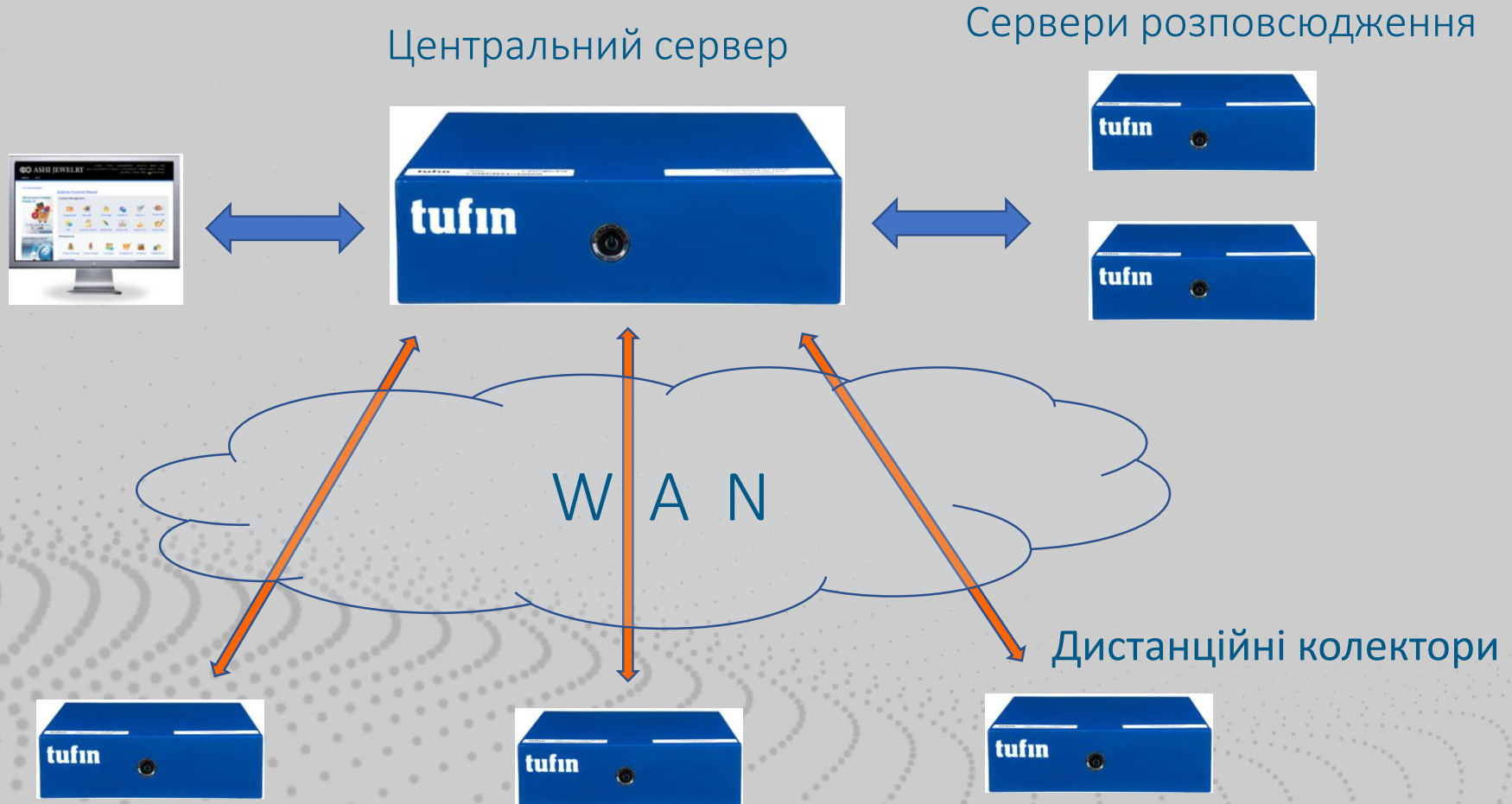
Logging: [Log](#)  
Comment: 'None'

**CISCO** All Commands

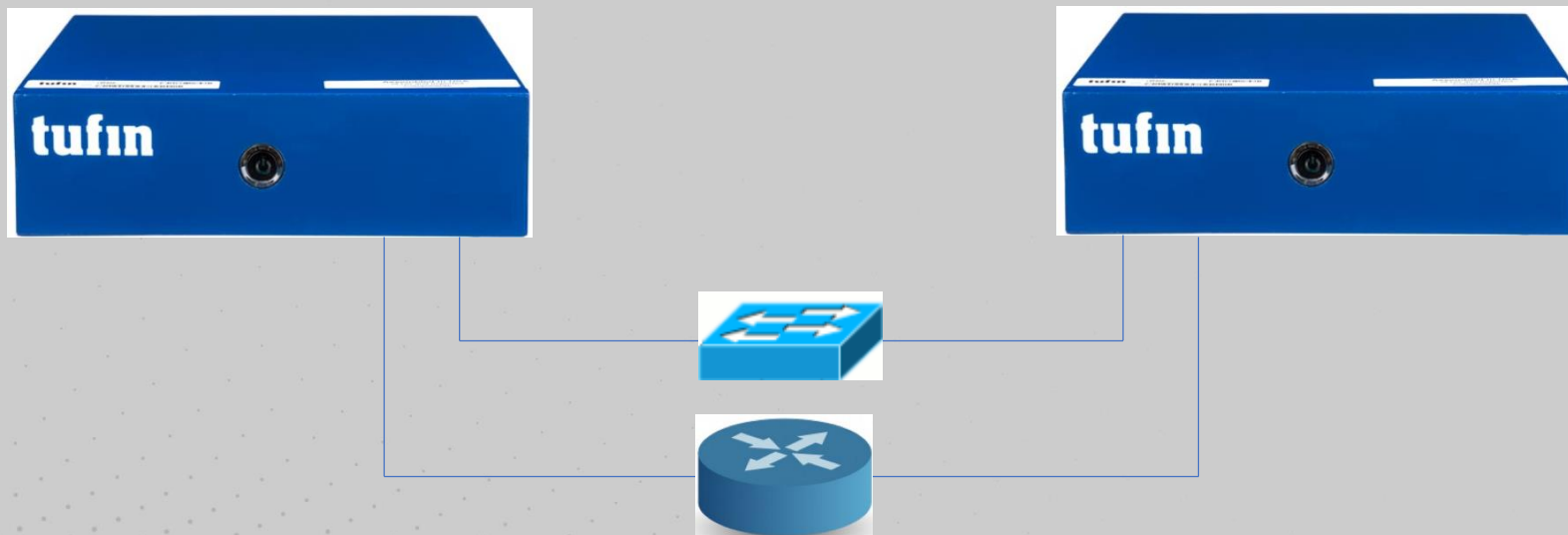
APPLICATIONS View: All applications  Show decommissioned applications New Application

Status	Name	Owner	Description	Created	Last Modified	Tickets
	<a href="#">3Rivers</a>	Henry Carr	Imported from Tetration	Thu, 14 Nov 2019	Thu, 14 Nov 2019	
	<a href="#">Access to CRM (Puppet)</a>	Henry Carr		Sun, 31 May 2015	Tue, 16 Jul 2019	
	<a href="#">Access to HQ (Via PAN Cluster)</a>	Henry Carr		Tue, 15 Mar 2016	Sun, 3 Mar 2019	2
	<a href="#">Access to RnD</a>	Henry Carr		Tue, 17 Apr 2018	Tue, 3 Sep 2019	3
	<a href="#">Access to Sales</a>	Tina White		Mon, 29 Jun 2015	Thu, 12 Sep 2019	6
	<a href="#">Access to Vmware ESX</a>	Tina White	FWs in path: ASA, Palo Alto, Srx	Wed, 18 Feb 2015	Wed, 2 May 2018	3
	<a href="#">ACI Fabric-Design-Team/App-1</a>	Henry Carr		Wed, 26 Feb 2020	Wed, 26 Feb 2020	
	<a href="#">ACI Fabric-Topology-Team/APP-Topology-Team</a>	Henry Carr		Mon, 2 Dec 2019	Mon, 2 Dec 2019	
	<a href="#">ACI Fabric-Topology-Team/appP MOCK_1</a>	Henry Carr		Mon, 2 Dec 2019	Mon, 2 Dec 2019	
	<a href="#">ACI Fabric-Topology-Team/appP MOCK_2</a>	Henry Carr		Mon, 2 Dec 2019	Mon, 2 Dec 2019	
	<a href="#">ACI Fabric-Topology-Team/appP MOCK_4</a>	Henry Carr		Mon, 2 Dec 2019	Mon, 2 Dec 2019	
	<a href="#">Active Directory</a>	Henry Carr	CP, ASA, Palo Alto	Wed, 18 Feb 2015	Tue, 13 Feb 2018	5
	<a href="#">Application 100 - GeoVision Access</a>	Henry Carr	FWs in path: ASA, Palo Alto	Wed, 17 Jun 2015	Mon, 29 Feb 2016	1
	<a href="#">application 105 - AWS access</a>	Henry Carr	FWs in path:CP, ASA, Palo Alto	Wed, 17 Jun 2015	Thu, 26 Jul 2018	1
	<a href="#">Application 210 - File Tranfer</a>	Henry Carr	FWs in path - Palo Alto	Mon, 21 Sep 2015	Tue, 13 Feb 2018	1
	<a href="#">applicationDiscovery</a>	Henry Carr	With Connections & Map	Wed, 2 Mar 2016	Mon, 30 May 2016	1
	<a href="#">Applications Templates</a>	Henry Carr	Company applications templates, do not change without admin authori...	Sun, 8 Mar 2015	Mon, 9 Dec 2019	
	<a href="#">Cloud Templates</a>	Carl Garcia		Wed, 18 Mar 2015	Tue, 8 Mar 2016	
	<a href="#">Company WEB Site - On-AWS</a>	Henry Carr		Tue, 8 Mar 2016	Sun, 3 Mar 2019	
	<a href="#">Company WEB Site - On Physical Site</a>	Jack Thomas	FWs in path: ASA, CP	Mon, 23 Feb 2015	Tue, 8 Mar 2016	2
	<a href="#">Connection-analysis-with-AWS</a>	Henry Carr	AWS Security-Group-allowing-the-traffic	Sun, 6 Mar 2016	Sun, 3 Mar 2019	1
	<a href="#">Credit Cards Analytics</a>	Henry Carr	FWs in path: ASA, CP	Tue, 10 Mar 2015	Mon, 16 May 2016	3
	<a href="#">Customer Analytics</a>	Tina White	FWs in path: Palo alto	Mon, 29 Dec 2014	Mon, 12 Sep 2016	2
	<a href="#">DC Replication - NSX (Physical to Hybrid)</a>	Carl Garcia	FWs in path: ASA, SRX, NSX	Wed, 18 Mar 2015	Sun, 28 Jun 2015	
	<a href="#">Decommission 01 - Remove Server From Group</a>	Carl Garcia		Mon, 29 Jun 2015	Mon, 21 Sep 2015	1
	<a href="#">Decommission 02 - Simple rule removal</a>	Henry Carr	FWs in path: ASA, CP	Wed, 17 Jun 2015	Thu, 2 Jul 2015	
	<a href="#">Decommission 03 - Remove a Service</a>	Jack Thomas	FWs in path: Stonesoft, ASA, Palo Alto	Mon, 29 Jun 2015	Sun, 19 Jul 2015	
	<a href="#">DNS server</a>	Henry Carr		Mon, 9 Dec 2019	Mon, 16 Dec 2019	1
	<a href="#">Fraud Monitoring 01</a>	Henry Carr	Monitor Mail service vulnerability - must stay disconnected !	Tue, 10 Mar 2015	Thu, 2 Apr 2015	

Evaluation license (for Tufin RnD) expires in 50 day(s) | [Refresh license status](#)



- ✓ Завдання: отримання оновлень, аналіз політик після отримання, формування звітів



- ✓ Архітектура «Active» – «Hot Standby»
- ✓ Між: ПАК-ПАК, VM-VM, ПАК-VM
- ✓ Інтерфейс Heartbeat-повідомлень – Layer 2
- ✓ Інтерфейс обміну даними – Layer 3

# Tufin Software Technologies - ключовий вендор Unified Firewalls Management



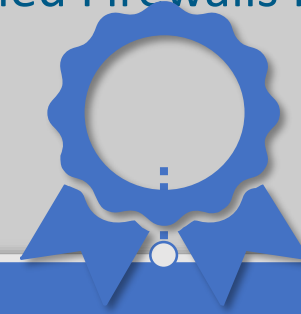
>2000

клієнтів  
в 50 країнах



Поєднання:

- Аналітика
- Процеси
- Додатки



- Ізраїльська компанія
- Заснована в 2005 році



Дякую за увагу!

Денис Фомкін  
м. +38 050 330-38-33  
[dfomkin@nwu.com.ua](mailto:dfomkin@nwu.com.ua)  
[nwu.com.ua](http://nwu.com.ua)