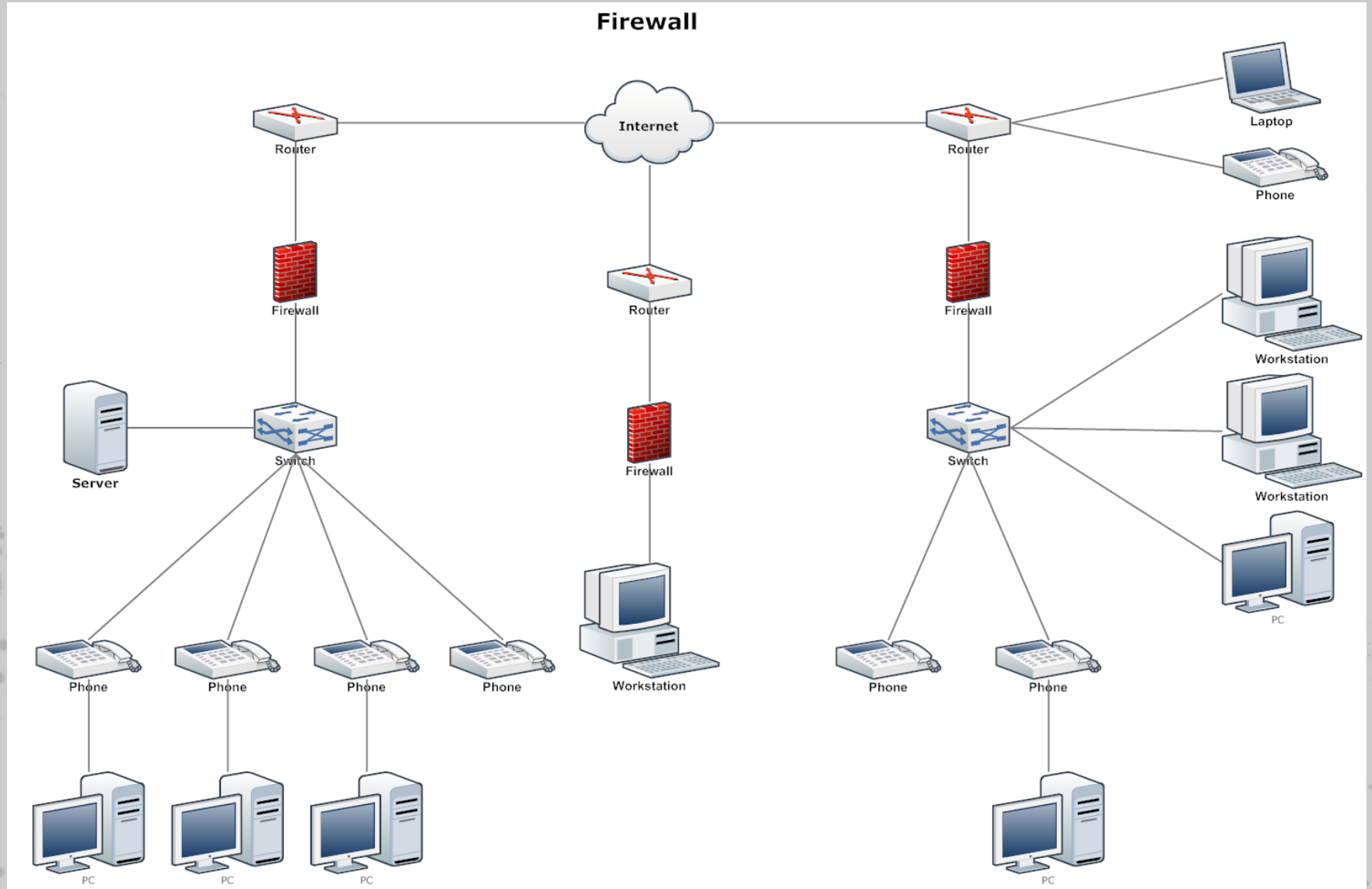
2020

Фаєрволи. Просте управління складними рішеннями

Денис Фомкін
nwu.com.ua


Firewall
Internet
Router
Router
Laptop
Phone
Firewall
Router
Firewall
Workstation
Server
Switch
Firewall
Switch
Workstation
Phone
Phone
Phone
Phone
Workstation
Phone
Phone
PC
PC
PC
PC

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:

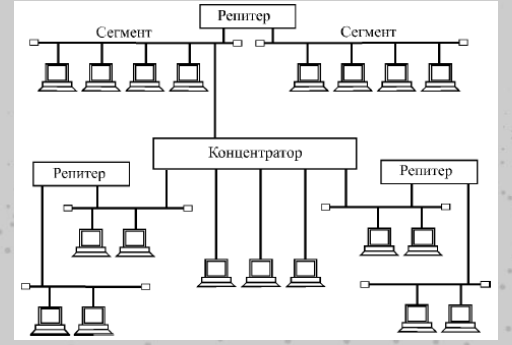
- Дублюючі, затінюючі, невикористовувані об'єкти і правила
- Фактичне використання правил - оптимізація

✓ 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 ME

✓ 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
- ✓ IT- підрозділи, мережеві фахівці, сисадміни

Функціонал, що не надається консолями ЦК окремих виробників

SecureChange

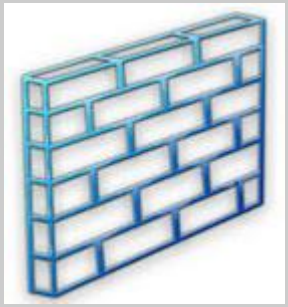
- ✓ Формування та обробка додатків для доступу в Інтернет
- ✓ Дизайн, аналіз ризиків і безпеки
- ✓ ІБ підрозділи, а не технічний персонал

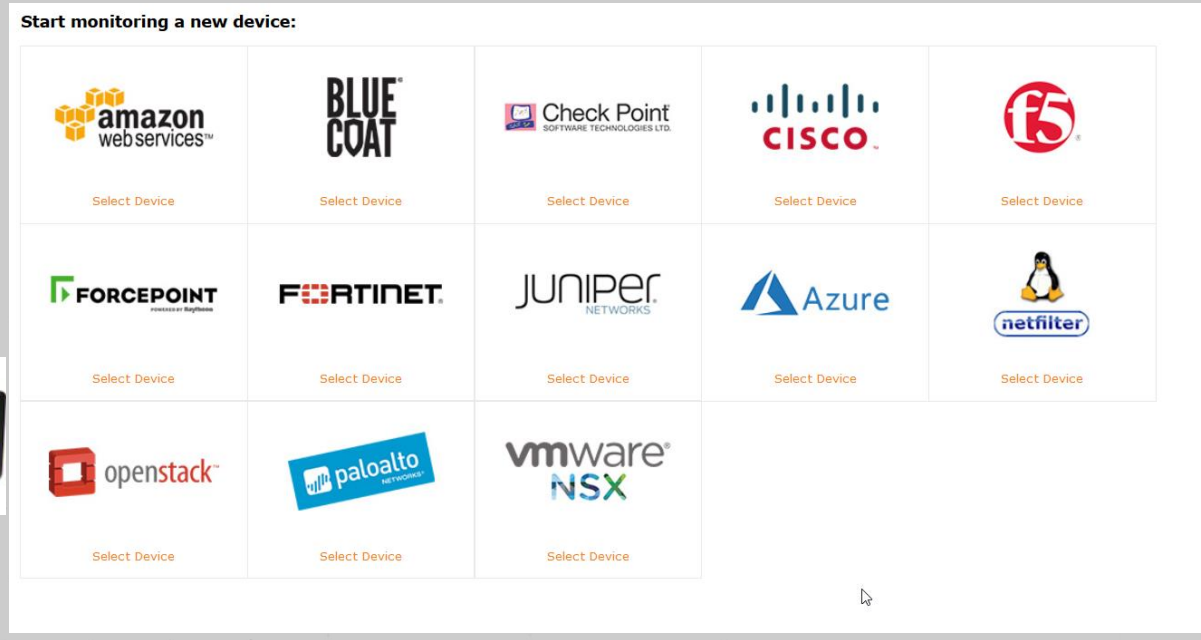
Процеси доступу до бізнесу, Автоматизація впровадження, оцінка безпеки

SecureApp

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

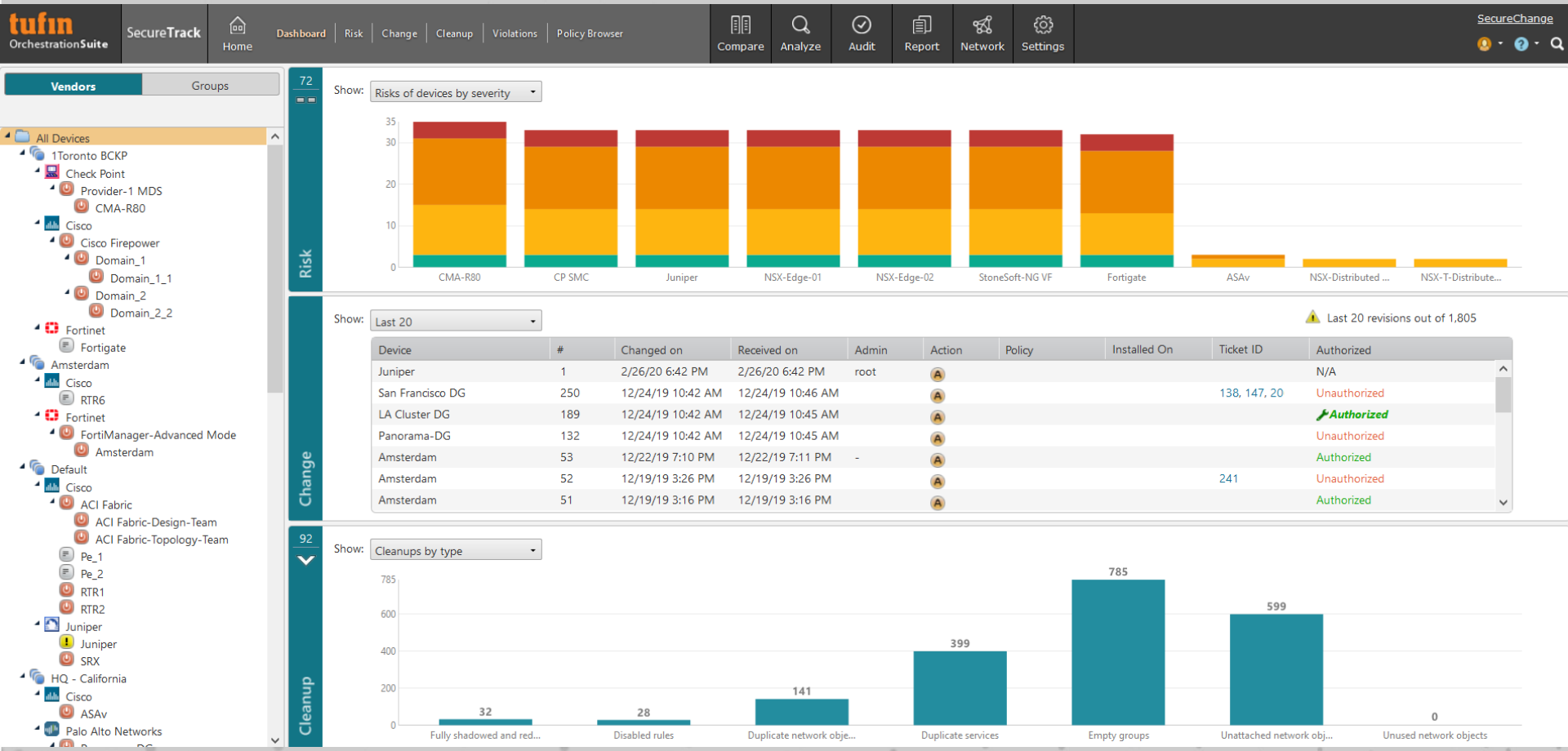
Модуль захисту доступу для критичних додатків



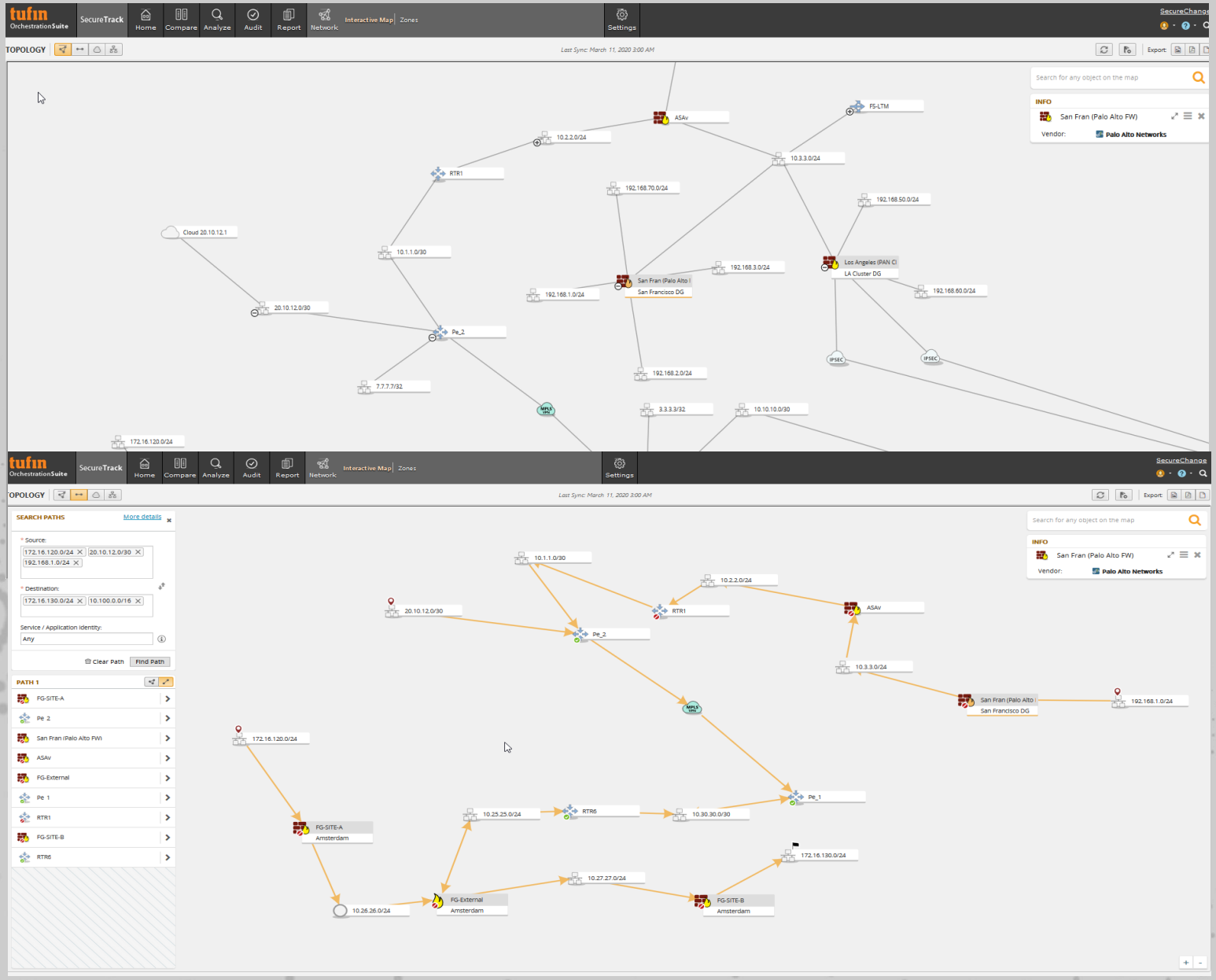


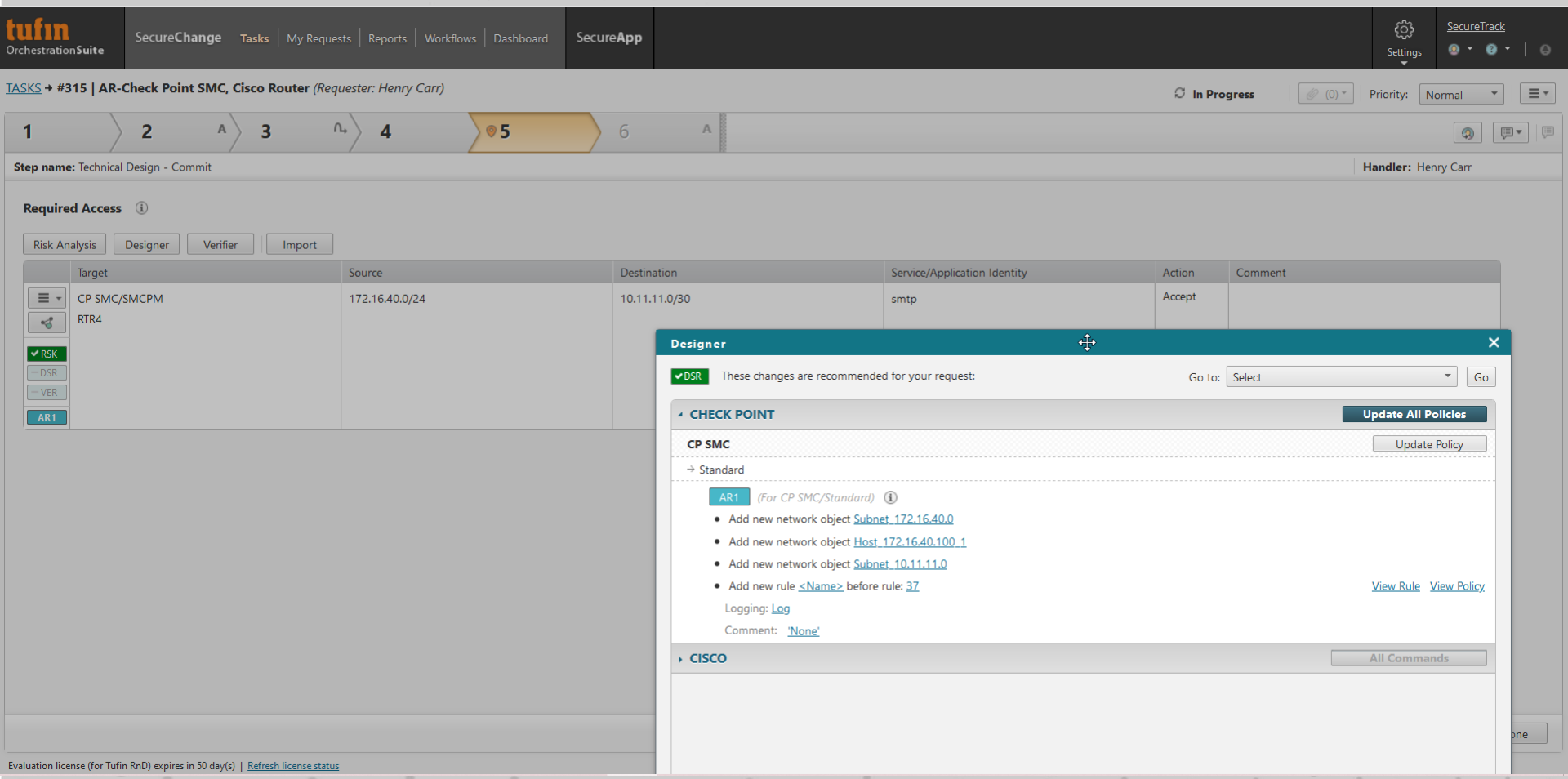
- ✓ Підтримка керуючих консолей та окремих пристроїв від провідних постачальників: Juniper, Palo Alto (PA – Services/Users), Cisco, Fortinet, McAfee, Stonesoft, BlueCoat, F5 BIG IP та інші...
- ✓ Все, що Linux/Unix на основі IPTables
- ✓ Комутатори, NLB, Generic Type, хмарні ресурси

Tufin Secure Track

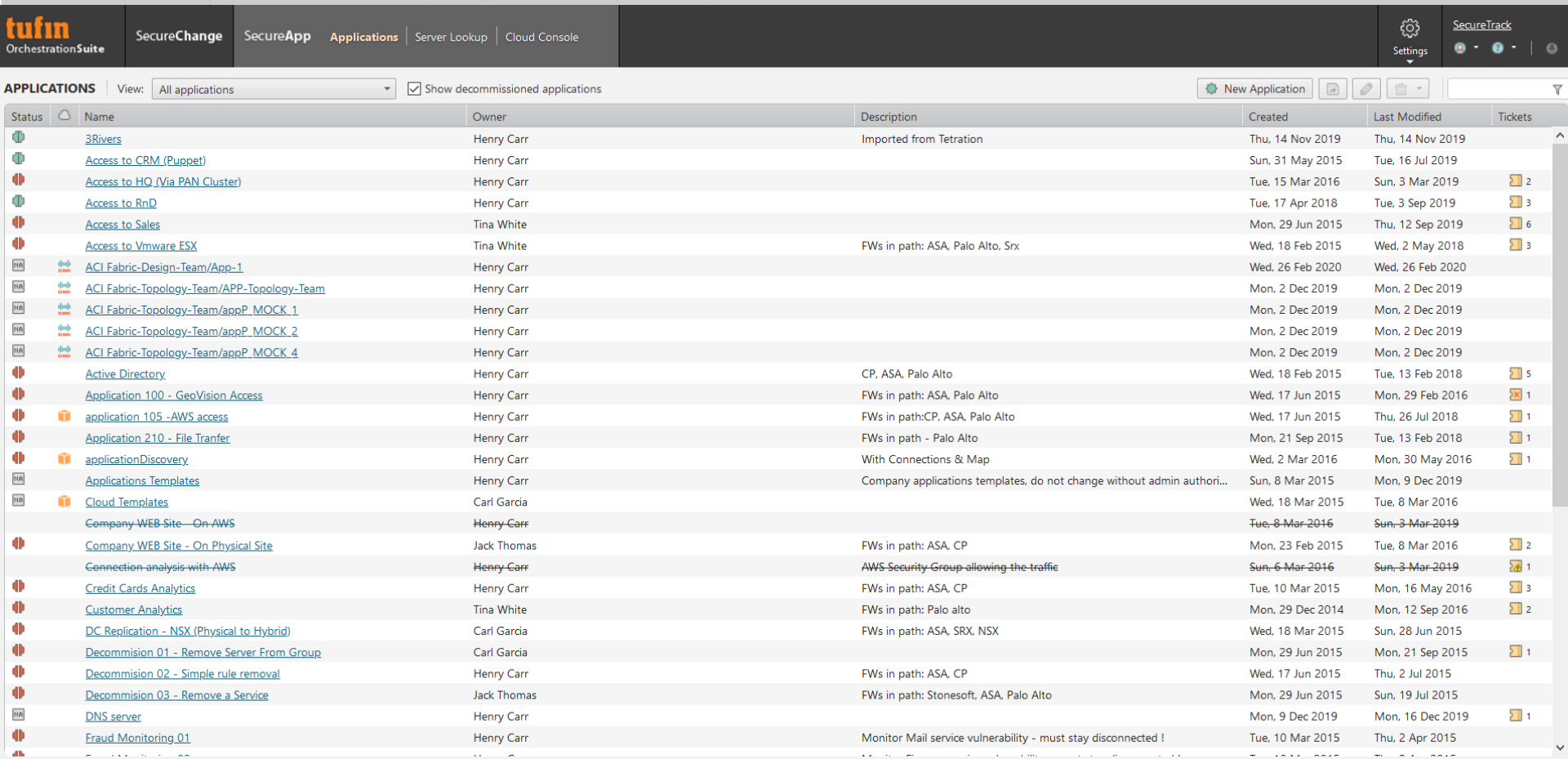


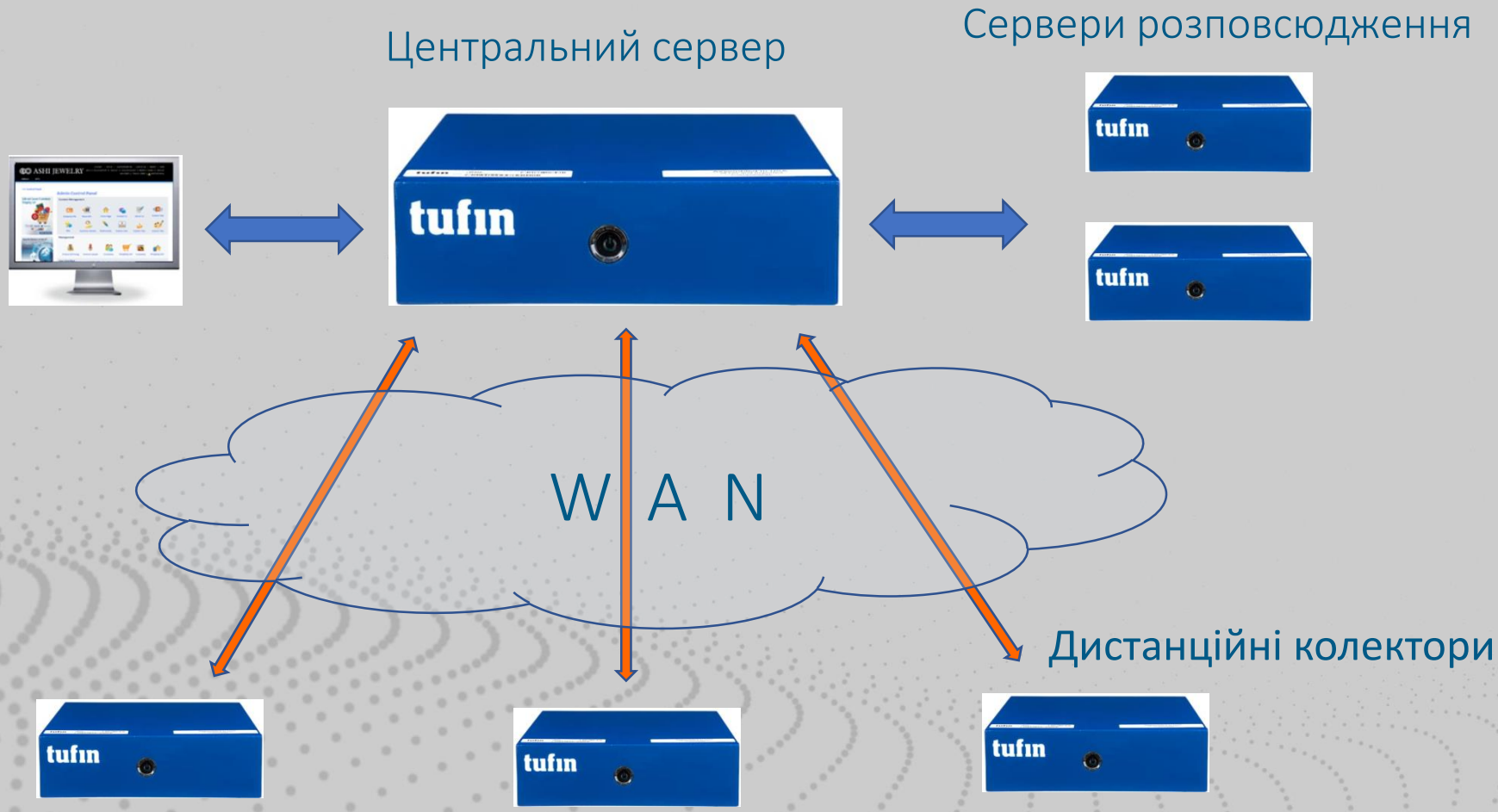
Tufin Secure Track



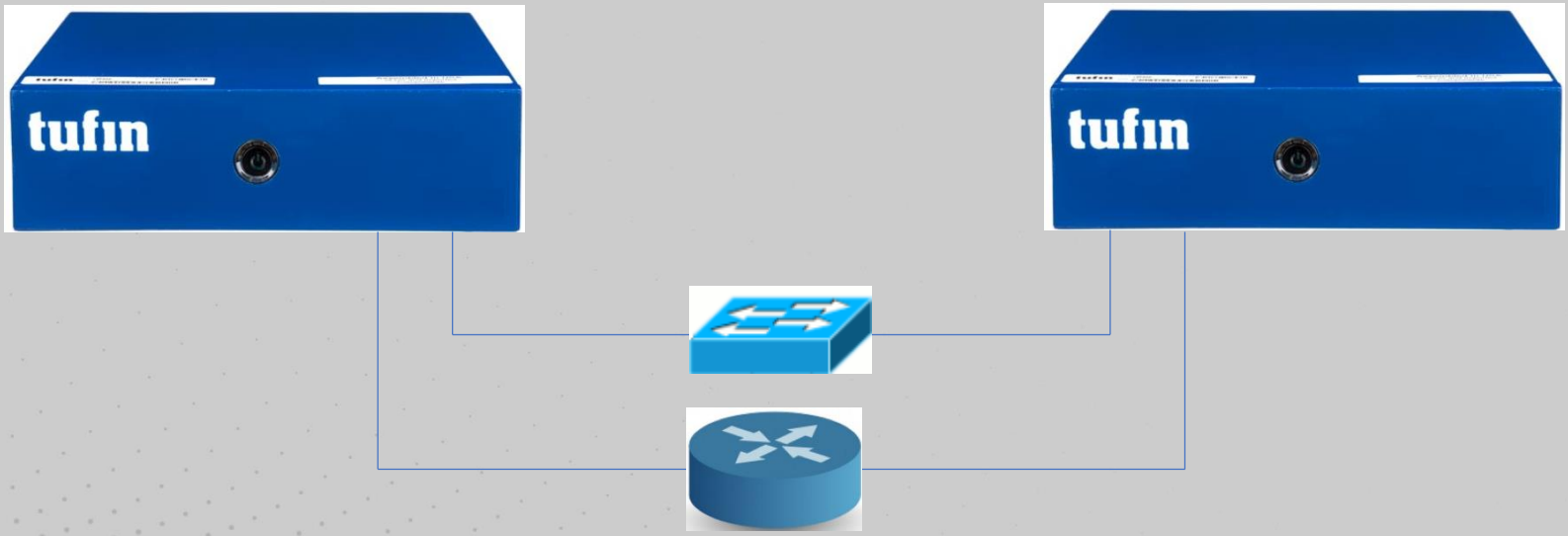

tufin OrchestrationSuite
SecureChange
Tasks
My Requests
Reports
Workflows
Dashboard
SecureApp
Settings
SecureTrack
TASKS → #315 | AR-Check Point SMC, Cisco Router (Requester: Henry Carr)
In Progress
Priority: Normal
1
2
3
4
5
6
Step name: Technical Design - Commit
Handler: Henry Carr
Required Access
Risk Analysis
Designer
Verifier
Import
Target
Source
Destination
Service/Application Identity
Action
Comment
CP SMC/SMCPM
RTR4
172.16.40.0/24
10.11.11.0/30
smtp
Accept
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
Evaluation license (for Tufin RnD) expires in 50 day(s) | Refresh license status

Tufin Secure App





- ✓ 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
nwu.com.ua