

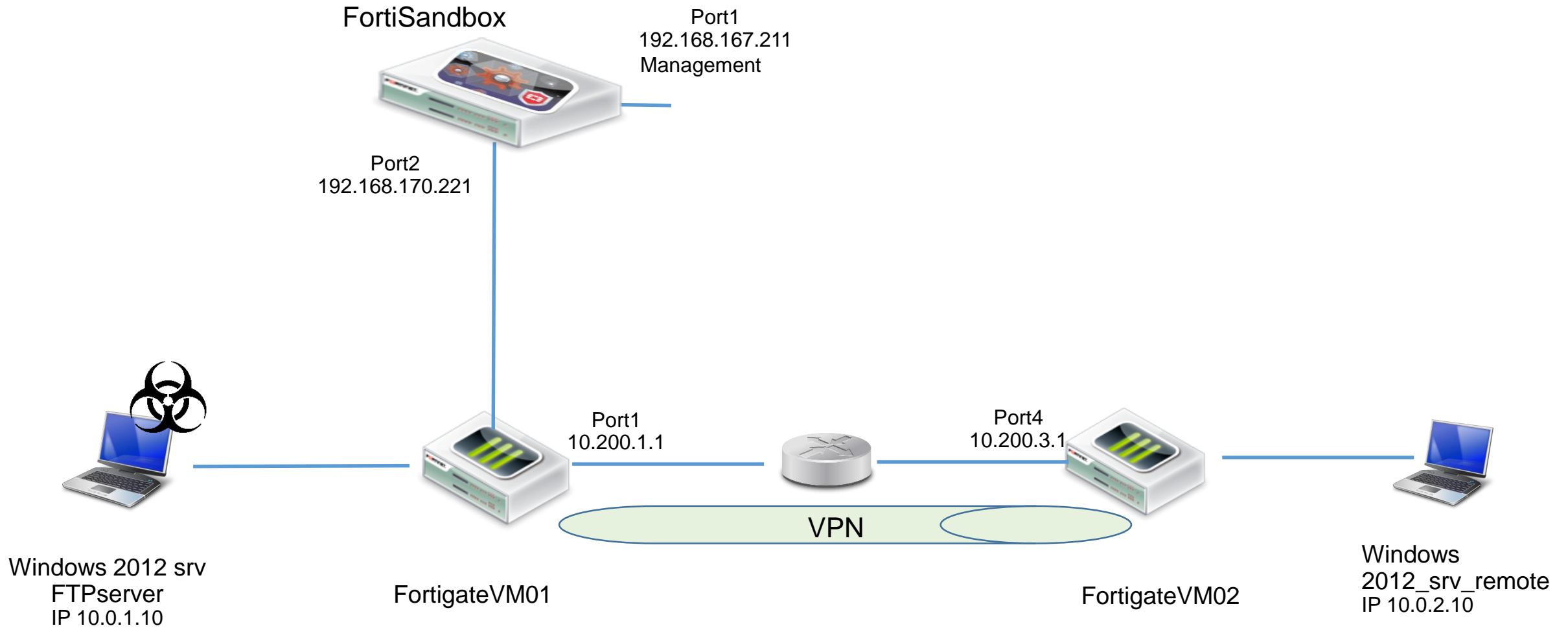


**EXCLUSIVE
NETWORKS**

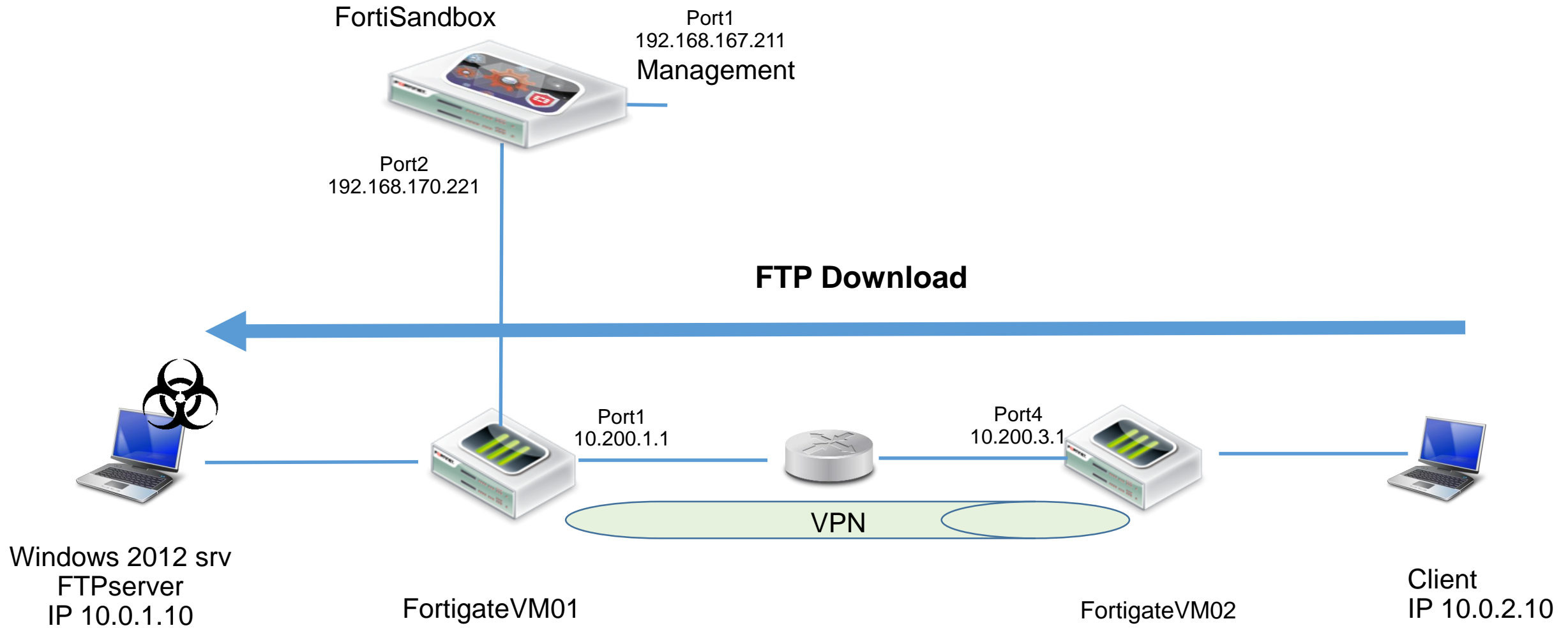
**Visibilità, controllo e sicurezza as a service:
l'efficacia di un framework integrato contro le
minacce di nuova generazione**

**Heros Deidda,
System Engineer Exclusive-Networks**

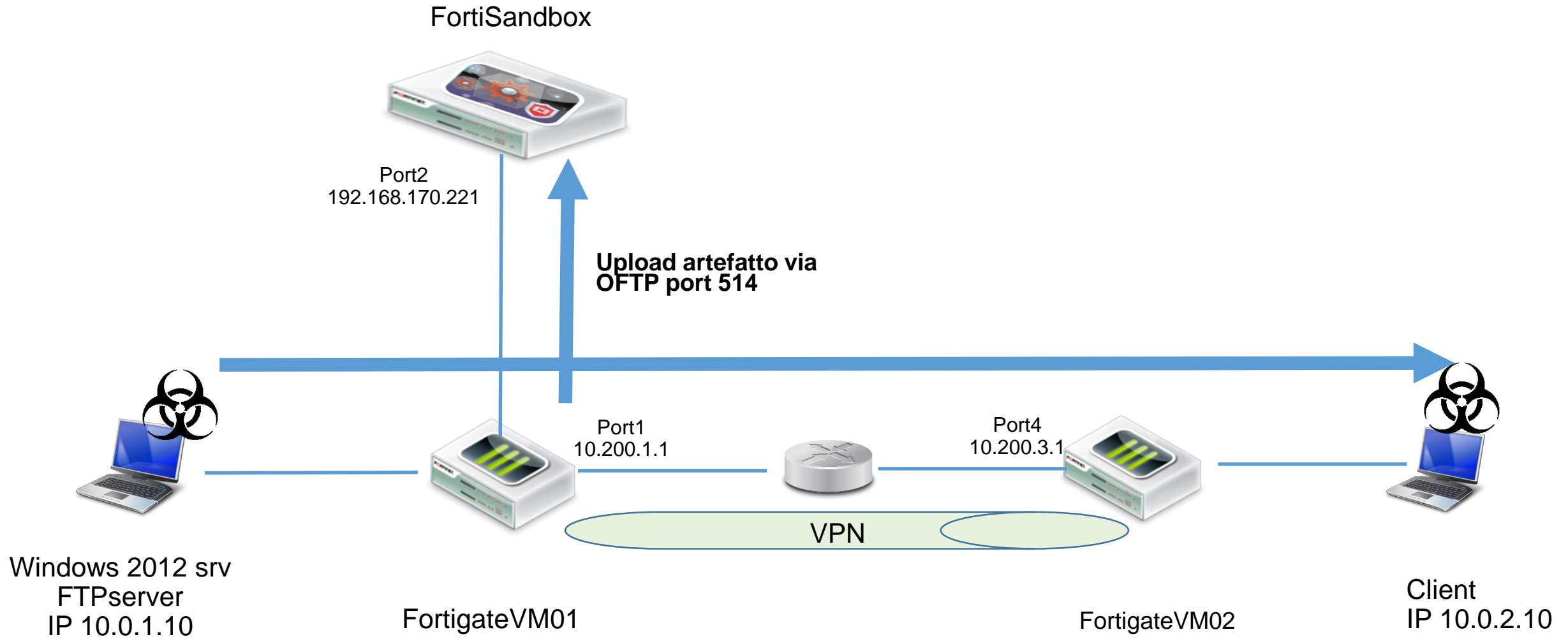
Lab TechExperience: Integrazione Fortigate FortiSandbox



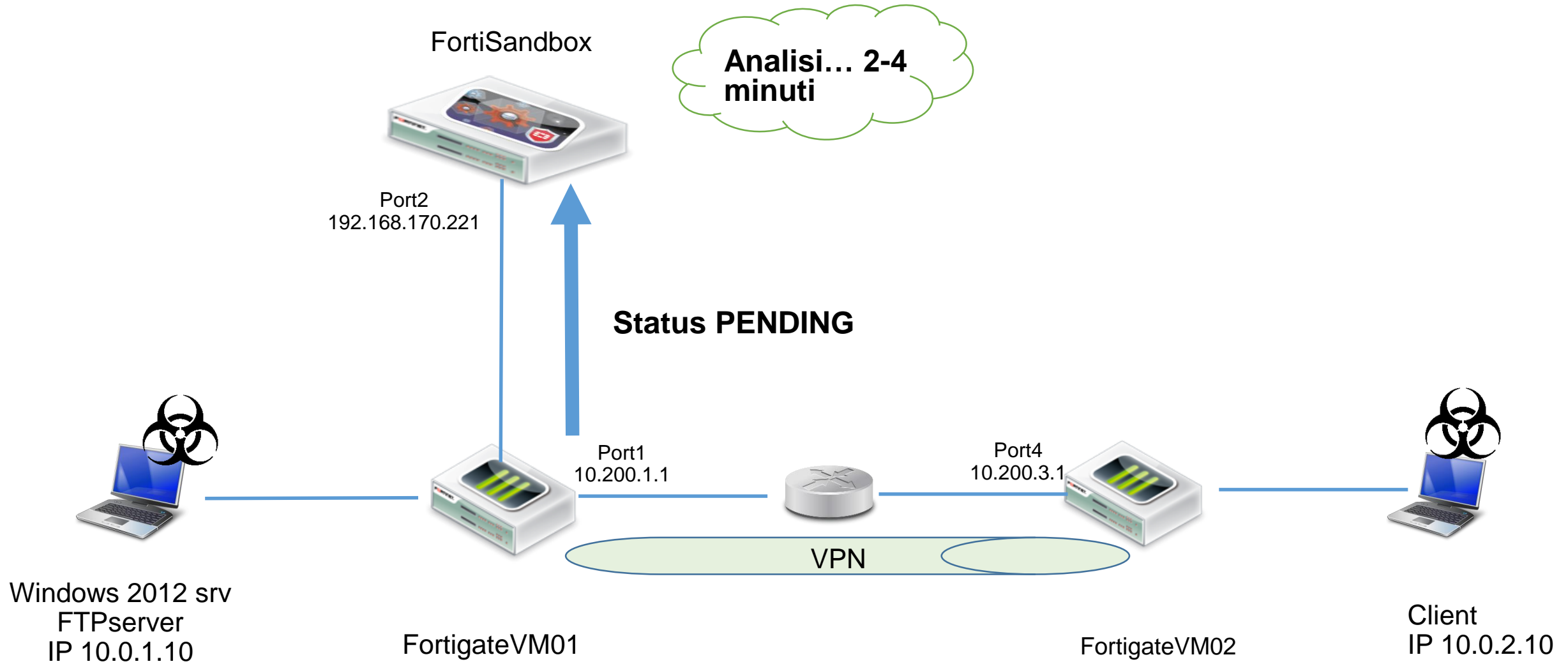
Lab TechExperience: Integrazione Fortigate FortiSandbox



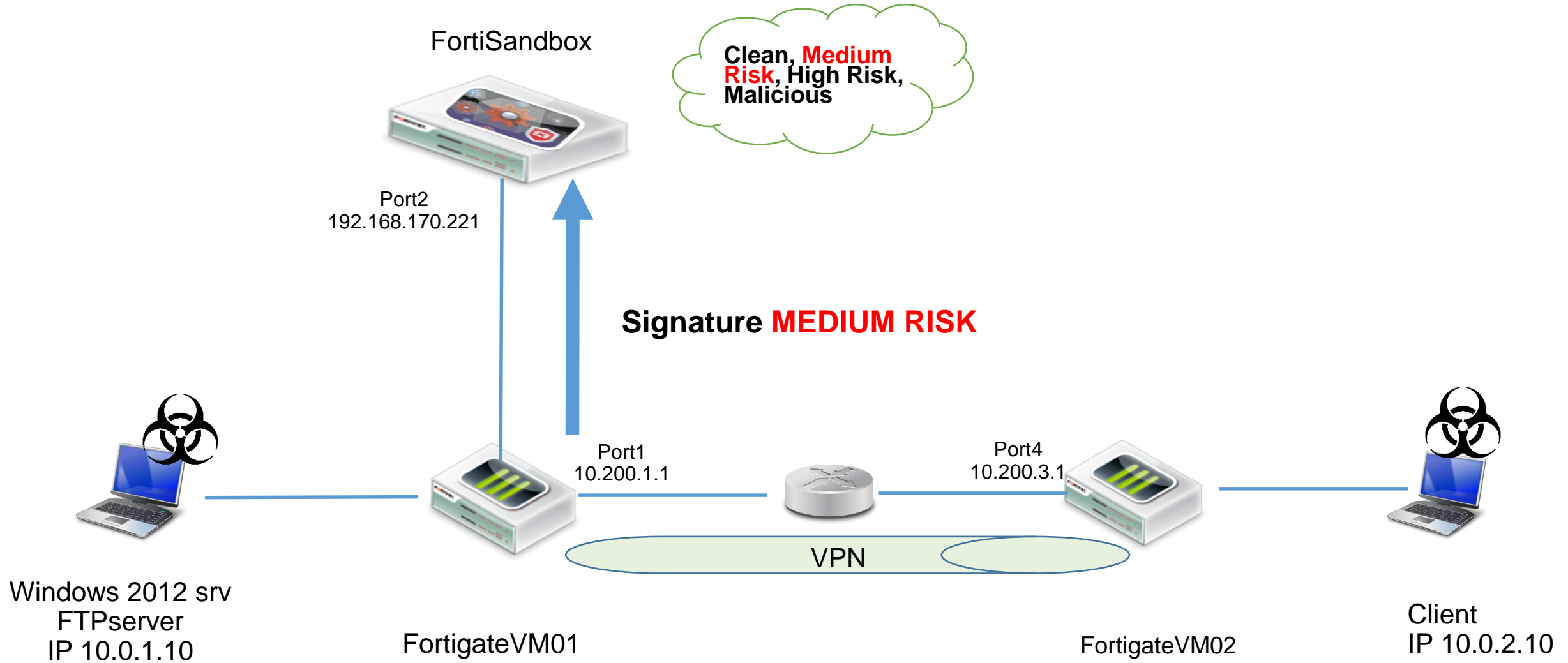
Lab TechExperience: Integrazione Fortigate FortiSandbox



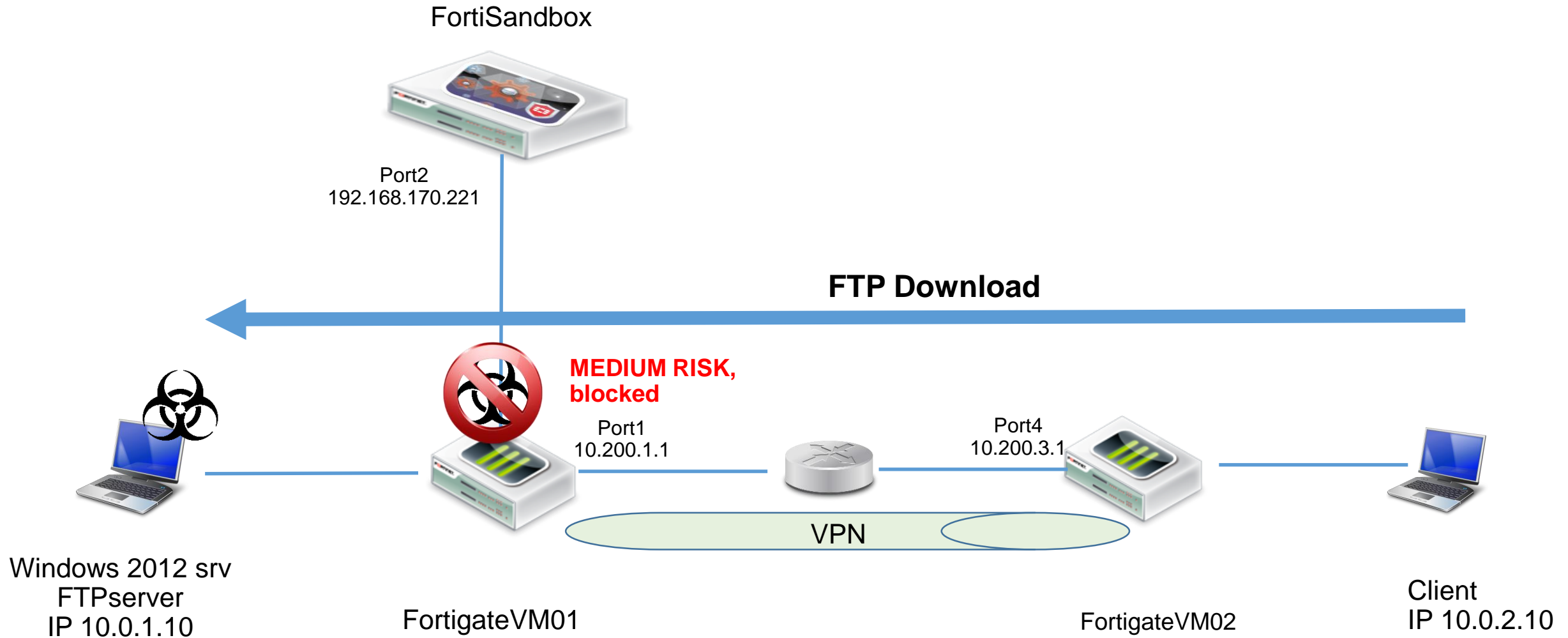
Lab TechExperience: Integrazione Fortigate FortiSandbox



Lab TechExperience: Integrazione Fortigate FortiSandbox



Lab TechExperience: Integrazione Fortigate FortiSandbox



Configurazione: Fortigate

Lab TechExperience: Integrazione Fortigate FortiSandbox

The screenshot displays the FortiGate VM Student interface. The left sidebar contains a navigation menu with the following items: Dashboard, FortiView, Network, System (highlighted), Administrators, Admin Profiles, Settings, HA, SNMP, Replacement Messages, FortiGuard, External Security Devices (highlighted), Advanced, Feature Select, Certificates, Policy & Objects, Security Profiles, VPN, User & Device, WiFi Controller, and Log & Report. The main content area is titled 'External Security Devices' and includes the following configuration options:

- HTTP Service
- SMTP Service - FortiMail
- Enable sandbox inspection

Below these options, there are two tabs: 'FortiSandbox Appliance' (selected) and 'FortiSandbox Cloud'. The 'FortiSandbox Appliance' configuration includes:

- Server: 192.168.170.221 (with a 'Test Connectivity' button)
- Notifier Email: (empty text input field)

Under the 'Applied Threat Intelligence' section, there are two rows of data:

Dynamic Malware Detection version	2.111 (signatures: 3)
URL Threat Detection version	2.100 (entries: not loaded)

At the bottom, the 'FortiSandbox statistics (last 7 days)' section contains a table:

File type	Detected
Total submitted	6
Malicious	2
Suspicious (high risk)	0
Suspicious (medium risk)	2
Suspicious (low risk)	0
Clean	2

Lab TechExperience: Integrazione Fortigate FortiSandbox

The screenshot displays the FortiGate VM Student interface. The left sidebar contains a navigation menu with the following items: Dashboard, FortiView, Network, System, Policy & Objects, Security Profiles (expanded), AntiVirus (selected), Web Filter, DNS Filter, Application Control, Cloud Access Security Inspection, Intrusion Protection, FortiClient Profiles, Proxy Options, SSL/SSH Inspection, Web Rating Overrides, Web Profile Overrides, VPN, User & Device, WiFi Controller, and Log & Report. The main content area is titled "Edit AntiVirus Profile" and includes the following configuration options:

- Name: default
- Comments: scan and delete virus (21/255)
- Detect Viruses: Block (selected), Monitor
- Inspected Protocols:
 - HTTP:
 - SMTP:
 - POP3:
 - IMAP:
 - MAPI:
 - FTP:
 - NNTP:
- Inspection Options:
 - Treat Windows Executables in Email Attachments as Viruses:
 - Send Files to FortiSandbox Appliance for Inspection:
 - File Selection: Suspicious Files Only, Executable Files Only, All Supported Files (selected)
 - Use FortiSandbox Database:
 - Include Mobile Malware Protection:

An "Apply" button is located at the bottom right of the configuration area.

Configurazione: FortiSandbox

Lab TechExperience: Integrazione Fortigate FortiSandbox

FortiSandbox VM ? admin

Search Edit

- Dashboard
- FortiView
- Network
 - Interfaces**
 - System DNS
 - System Routing
- System
- Virtual Machine
- Scan Policy
- Scan Input
- File Detection
- Network Alerts
- URL Detection
- Log & Report

Interface	IPv4	IPv6	Interface Status	Link Status	Access Rights
port1 (administration port)	192.168.167.211/255.255.255.0				HTTPS,HTTP,SSH,TELNET
port2	192.168.170.221/255.255.255.0				
port3 (VM outgoing port)	192.168.169.211/255.255.255.0				
port4	192.168.3.99/255.255.255.0				
port5	192.168.4.99/255.255.255.0				
port6	192.168.5.99/255.255.255.0				

6 Network interfaces

Lab TechExperience: Integrazione Fortigate FortiSandbox

FortiSandbox VM ? [Fullscreen] admin ▾

Search:

[Edit](#) [Delete](#) [Malware Packages](#) [URL Packages](#)

Device Name	Serial	Malicious	High	Medium	Low	Clean	Unknown	Malware Pkg	URL Pkg	Authorized	
Student	FGVM010000016890	2	0	2	0	2	0	2.112	2.100		
Student:root	FGVM010000016890	2	0	2	0	2	0	2.112	2.100		

Navigation: 30 | Page 1 of 1 | Displaying 1 to 2 of 2 Device(s) | Last 7 Days

- Dashboard
- FortiView
- Network
- System
- Virtual Machine
- Scan Policy
- Scan Input**
 - File On-Demand
 - URL On-Demand
- Device**
 - FortiClient
 - Adapter
 - Network Share
 - Quarantine

Lab TechExperience: Integrazione Fortigate FortiSandbox

FortiSandbox VM ? admin

Dashboard
FortiView
Network
System
Virtual Machine
Scan Policy
Scan Input
File On-Demand
URL On-Demand
Sniffer
Device
FortiClient
Adapter

Delete Malware Packages URL Packages

FCT Serial	Hostname	IP	Malicious	High Risk	Medium Risk	Low Risk	Clean	Unknown Risk	Malware Pkg	URL Pkg	
FCT8000723293965	ROBBYN-7	192.168.167.254	0	0	0	0	24	0	N/A	N/A	r.narettc
FCT8002240007845	THINKPAD	192.168.170.254	0	0	0	0	4	0	N/A	N/A	enghell
FCT8002409642643	REMOTE	192.168.170.254	3	0	6	0	3	1	N/A	N/A	Adminis

Analisi: Vista Fortisandbox

Lab TechExperience: Integrazione Fortigate FortiSandbox

The screenshot displays the FortiSandbox VM interface. At the top, a green header bar contains the FortiSandbox logo, the text "VM", a help icon, a full-screen icon, and the user name "admin". Below the header is a navigation menu on the left with the following items: Dashboard, FortiView, Network, System, Virtual Machine (expanded), VM Status (highlighted), VM Images, Scan Policy, Scan Input, File Detection, Network Alerts, URL Detection, and Log & Report. The main content area shows a file upload progress bar for the file "77a520df83df59af0767f167662b2c0d4d54a31eb73002c6aa03b073ad30f5ca.exe". The progress bar is currently at 41.67%.

File	Progress
77a520df83df59af0767f167662b2c0d4d54a31eb73002c6aa03b073ad30f5ca.exe	41.67%

Lab TechExperience: Integrazione Fortigate FortiSandbox

The screenshot displays the FortiSandbox VM web interface. The top navigation bar is green and contains the FortiSandbox logo, the text 'VM', a help icon, a full-screen icon, and the user 'admin'. Below the navigation bar is a search and filter area with a 'Last 24 Hours' dropdown, an 'Export Data' button, a search toggle, and a 'Filter ...' input field. A left-hand sidebar menu lists various sections: Dashboard, FortiView, Network, System, Virtual Machine, Scan Policy, Scan Input, File Detection (highlighted), Network Alerts, URL Detection, and Log & Report. Under 'File Detection', sub-items include Summary Report, Malicious Files, Suspicious Files (highlighted), and Clean/Unknown Files. The main content area shows a table with one data row. The table headers are: Detected, Type, Rating, Source, Destination, Domain, and Infected OS. The data row shows: May 16 2016 16:59:08, Unknown, Medium Risk (with a warning icon), 10.0.2.10, 10.0.1.10, N/A, and WINXPVM1.

Detected	Type	Rating	Source	Destination	Domain	Infected OS
May 16 2016 16:59:08	Unknown	Medium Risk	10.0.2.10	10.0.1.10	N/A	WINXPVM1

Lab TechExperience: Integrazione Fortigate FortiSandbox

The screenshot displays the FortiSandbox VM interface. On the left is a navigation menu with categories like Dashboard, FortiView, Network, System, Virtual Machine, Scan Policy, Scan Input, File Detection, and Log & Report. The 'File Detection' section is expanded, showing 'Suspicious Files' as the active view. The main area shows a detected file from May 16, 2016, at 16:59:08. A modal window titled 'Medium Risk Unknown' is open, providing detailed analysis. The 'Behavior Summary' section lists several actions: network traffic, dropping files, deleting files, hiding windows, and spawning processes. The 'Analysis Details' section shows the file type as 'exe' and that it was downloaded from an unknown source. At the bottom of the modal, there are tabs for 'WIN7X64VM' and 'WINXPVM1', and buttons to download 'Captured Packets', 'Original File', 'Tracer Package', and 'Tracer Log'. A 'Behavior Chronology Chart' is also present but currently empty.

Medium Risk Unknown

- More Details
- Behavior Summary
 - This file has network traffic
 - This file dropped files
 - This file deleted files
 - This file had no window or its main window is hidden
 - This file spawned process(es)
- Analysis Details
 - Packer: N/A
 - File Type: exe
 - Downloaded From: N/A

WIN7X64VM | WINXPVM1

Captured Packets | Original File | Tracer Package | Tracer Log

Behavior Chronology Chart

Analisi: Fortigate

Lab TechExperience: Integrazione Fortigate FortiSandbox

FortiGate VM Student admin ▾

Dashboard FortiView Sources Destinations Interfaces Policies Countries WiFi Clients Device Topology Traffic Shaping All Sessions Applications Cloud Applications Web Sites Threats Threat Map **FortiSandbox** Failed Authentication System Events Admin Logins VPN

Refresh Add Filter Files Source 5 minutes **1 hour** 24 hours ⚙️

Source	File Name	Status	Submitted
10.0.2.10	57a2636a6fcd67a69a7c8ec15d5c496a4f4bde748cb71034c1836ff12d4cc22d (1).exe	Medium	05/16/2016 14:40:00
10.0.2.10	77a520df83df59af0767f167662b2c0d4d54a31eb73002c6aa03b073ad30f5ca.exe	Clean	05/16/2016 14:30:00
10.0.2.10	77a520df83df59af0767f167662b2c0d4d54a31eb73002c6aa03b073ad30f5ca.exe	Clean	05/16/2016 14:48:00
10.0.2.10	putty.exe	Clean	05/16/2016 14:48:00

Lab TechExperience: Integrazione Fortigate FortiSandbox

FortiGate VM Student admin

Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
WiFi Controller
Log & Report
Forward Traffic
Local Traffic
System Events
VPN Events
WiFi Events
AntiVirus
Local Reports
Log Settings
Threat Weight
Monitor

Log location: D

#	@	Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
1		05-16 14:48	FTP	10.0.2.10	d6af33ce2ad3e43c62efefb4d1c8bdc270b0b4340877dd10502453fe9c1d03a8.exe	FSA/RISK_MALICIOUS		host: 10.0.1.10	blocked
2		05-16 14:47	FTP	10.0.2.10	d6af33ce2ad3e43c62efefb4d1c8bdc270b0b4340877dd10502453fe9c1d03a8 (1).exe	FSA/RISK_MALICIOUS		host: 10.0.1.10	blocked
3		05-16 14:47	FTP	10.0.2.10	77a520df83df59af0767f167662b2c0d4d54a31eb73002c6aa03b073ad30f5ca.exe			host: 10.0.1.10	analytics
4		05-16 14:47	FTP	10.0.2.10	putty.exe			host: 10.0.1.10	analytics
5		05-16 14:45	FTP	10.0.2.10	d6af33ce2ad3e43c62efefb4d1c8bdc270b0b4340877dd10502453fe9c1d03a8.exe	FSA/RISK_MALICIOUS		host: 10.0.1.10	blocked
6		05-16 14:44	FTP	10.0.2.10	d6af33ce2ad3e43c62efefb4d1c8bdc270b0b4340877dd10502453fe9c1d03a8 (1).exe	FSA/RISK_MALICIOUS		host: 10.0.1.10	blocked
7		05-16 14:44	FTP	10.0.2.10	4f2e7f1af8899dd903fcf76be44b3b34cfb806274effc4b5ecaecab0a2f557a.exe	FSA/RISK_MALICIOUS		host: 10.0.1.10	blocked
8		05-16 14:44	FTP	10.0.2.10	57a2636a6fcd67a69a7c8ec15d5c496a4f4bde748cb71034c1836ff12d4cc22d (1).exe			host: 10.0.1.10	analytics
9		05-16 14:27	FTP	10.0.2.10	77a520df83df59af0767f167662b2c0d4d54a31eb73002c6aa03b073ad30f5ca.exe			host: 10.0.1.10	analytics
10		05-13 11:23	FTP	10.0.2.10	f8a7cdd2e3b5721861f92fb0278dc4d4fc836036c4e0d719acd1d6857c09d3c9.exe	FSA/RISK_MALICIOUS		host: 10.0.1.10	blocked
11		05-13 11:22	FTP	10.0.2.10	f8a7cdd2e3b5721861f92fb0278dc4d4fc836036c4e0d719acd1d6857c09d3c9.exe	FSA/RISK_MALICIOUS		host: 10.0.1.10	blocked
12		05-13 11:14	FTP	10.0.2.10	fb8075b026c3b72cb368a8341d0f9eb376da6ca83bf9489ecc2faa25c928411e.exe	FSA/RISK_MALICIOUS		host: 10.0.1.10	blocked
13		05-13 11:14	FTP	10.0.2.10	fb8075b026c3b72cb368a8341d0f9eb376da6ca83bf9489ecc2faa25c928411e.exe	FSA/RISK_MALICIOUS		host: 10.0.1.10	blocked
14		05-13 11:13	FTP	10.0.2.10	fb8075b026c3b72cb368a8341d0f9eb376da6ca83bf9489ecc2faa25c928411e.exe	FSA/RISK_MALICIOUS		host: 10.0.1.10	blocked
15		05-13 11:11	FTP	10.0.2.10	c82fec052692a235fc4abc3d86746d95d51ae448e8dc7987695b693504a5f6a.exe	W32/Swrort.C!tr		host: 10.0.1.10	blocked
16		05-13 11:08	FTP	10.0.2.10	c82fec052692a235fc4abc3d86746d95d51ae448e8dc7987695b693504a5f6a.exe	W32/Swrort.C!tr		host: 10.0.1.10	blocked
17		05-13 11:05	FTP	10.0.2.10	c82fec052692a235fc4abc3d86746d95d51ae448e8dc7987695b693504a5f6a.exe	W32/Swrort.C!tr		host: 10.0.1.10	blocked
18		05-13 10:54	FTP	10.0.2.10	c82fec052692a235fc4abc3d86746d95d51ae448e8dc7987695b693504a5f6a.exe	W32/Swrort.C!tr		host: 10.0.1.10	blocked
19		05-10 16:54	FTP	10.0.2.10	9abh52aa23f326a97ec6e1af41045d6c66f636d2533582b53b7d3fe035b247c4.exe			host: 10.0.1.10	analytics

1 / 1 [Total: 34]

#	8	Action	analytics
Date/Time	05-16 14:44	Destination	10.0.1.10
Destination	port3	Destination	21
Interface		Port	
Details	host: 10.0.1.10	Direction	incoming
Event Type	analytics	File Name	57a2636a6fcd67a69a7c8ec15d5c496a4f4bde748cb71034c1836ff12d4cc22d (1).exe

Lab TechExperience: Integrazione Fortigate FortiSandbox

FortiGate VM Student admin

Dashboard FortiView Network System Policy & Objects Security Profiles VPN User & Device WiFi Controller **Log & Report** Forward Traffic Local Traffic System Events VPN Events WiFi Events AntiVirus Local Reports Log Settings Threat Weight Monitor

Log location: Disk

#	@	Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
1		05-16 15:02	FTP	10.0.2.10	57a2636a6fcd67a69a7c8ec15d5c496a4f4bde748cb71034c1836ff12d4cc22d (1).exe	FSA/RISK_MEDIUM	host: 10.0.1.10		blocked
2		05-16 14:48	FTP	10.0.2.10	d6af33ce2ad3e43c62efefb4d1c8bdc270b0b4340877dd10502453fe9c1d03a8.exe	FSA/RISK_MALICIOUS	host: 10.0.1.10		blocked
3		05-16 14:47	FTP	10.0.2.10	d6af33ce2ad3e43c62efefb4d1c8bdc270b0b4340877dd10502453fe9c1d03a8 (1).exe	FSA/RISK_MALICIOUS	host: 10.0.1.10		blocked
4		05-16 14:47	FTP	10.0.2.10	77a520df83df59af0767f167662b2c0d4d54a31eb73002c6aa03b073ad30f5ca.exe		host: 10.0.1.10		analytics
5		05-16 14:47	FTP	10.0.2.10	putty.exe		host: 10.0.1.10		analytics
6		05-16 14:45	FTP	10.0.2.10	d6af33ce2ad3e43c62efefb4d1c8bdc270b0b4340877dd10502453fe9c1d03a8.exe	FSA/RISK_MALICIOUS	host: 10.0.1.10		blocked
7		05-16 14:44	FTP	10.0.2.10	d6af33ce2ad3e43c62efefb4d1c8bdc270b0b4340877dd10502453fe9c1d03a8 (1).exe	FSA/RISK_MALICIOUS	host: 10.0.1.10		blocked
8		05-16 14:44	FTP	10.0.2.10	4f2e7f1af8899d903fceff76be44b3b34cfb806274effc4b5ecaecab0a2f557a.exe	FSA/RISK_MALICIOUS	host: 10.0.1.10		blocked
9		05-16 14:44	FTP	10.0.2.10	57a2636a6fcd67a69a7c8ec15d5c496a4f4bde748cb71034c1836ff12d4cc22d (1).exe		host: 10.0.1.10		analytics
10		05-16 14:27	FTP	10.0.2.10	77a520df83df59af0767f167662b2c0d4d54a31eb73002c6aa03b073ad30f5ca.exe		host: 10.0.1.10		analytics
11		05-13 11:23	FTP	10.0.2.10	f8a7cdd2e3b5721861f92fb0278dc4d4fc836036c4e0d719acd1d6857c09d3c9.exe	FSA/RISK_MALICIOUS	host: 10.0.1.10		blocked
12		05-13 11:22	FTP	10.0.2.10	f8a7cdd2e3b5721861f92fb0278dc4d4fc836036c4e0d719acd1d6857c09d3c9.exe	FSA/RISK_MALICIOUS	host: 10.0.1.10		blocked
13		05-13 11:14	FTP	10.0.2.10	fb8075b026c3b72cb368a8341d0f9eb376da6ca83bf9489ecc2faa25c928411e.exe	FSA/RISK_MALICIOUS	host: 10.0.1.10		blocked
14		05-13 11:14	FTP	10.0.2.10	fb8075b026c3b72cb368a8341d0f9eb376da6ca83bf9489ecc2faa25c928411e.exe	FSA/RISK_MALICIOUS	host: 10.0.1.10		blocked
15		05-13 11:13	FTP	10.0.2.10	fb8075b026c3b72cb368a8341d0f9eb376da6ca83bf9489ecc2faa25c928411e.exe	FSA/RISK_MALICIOUS	host: 10.0.1.10		blocked
16		05-13 11:11	FTP	10.0.2.10	c82fec052692a235fc4abc3d86746d95d51ae448e8dc7987695b693504a5f6a.exe	W32/Swrort.C!tr	host: 10.0.1.10		blocked
17		05-13 11:08	FTP	10.0.2.10	c82fec052692a235fc4abc3d86746d95d51ae448e8dc7987695b693504a5f6a.exe	W32/Swrort.C!tr	host: 10.0.1.10		blocked
18		05-13 11:05	FTP	10.0.2.10	c82fec052692a235fc4abc3d86746d95d51ae448e8dc7987695b693504a5f6a.exe	W32/Swrort.C!tr	host: 10.0.1.10		blocked
19		05-13 10:54	FTP	10.0.2.10	c82fec052692a235fc4abc3d86746d95d51ae448e8dc7987695b693504a5f6a.exe	W32/Swrort.C!tr	host: 10.0.1.10		blocked

« < 1 /1 > » [Total: 35]

#	1	Action	blocked
Date/Time	05-16 15:02	Destination	10.0.1.10
Destination	port3	Destination	21
Interface		Port	
Details	host: 10.0.1.10	Detection Type	Virus
Direction	incoming	Event Type	infected
File Name	57a2636a6fcd67a69a7c8ec15d5c496a4f4bde748cb71034c1836ff12d4cc22d (1).exe	FortiSandbox	57a2636a6fcd67a69a7c8ec15d5c496a4f4bde748cb71034c1836ff12d4cc22d
Level	■■■■	Checksum	9234
Message	File reported infected by Sandbox.	Log ID	
		Policy	3



EXCLUSIVE
NETWORKS

Grazie

Heros Deidda
System Engineer, Exclusive Networks
hdeidda@exclusive-networks.com
cell 3492720440