Se prémunir des Cyberattaques grâce à la Fortinet Security Fabric

11.02.2021 | Chithavong Chokbengboun & Sylvain Pionchon

Nos Experts, vos accompagnateurs

Chithavong CHOKBENGBOUN

- Expérience de 7 ans dans l‘intégration de solution de sécurité
- Expert sécurité réseau
- Certifié Fortinet

Bechtle BU PS - Réseau et sécurité

Nos Experts, vos accompagnateurs

Sylvain PIONCHON

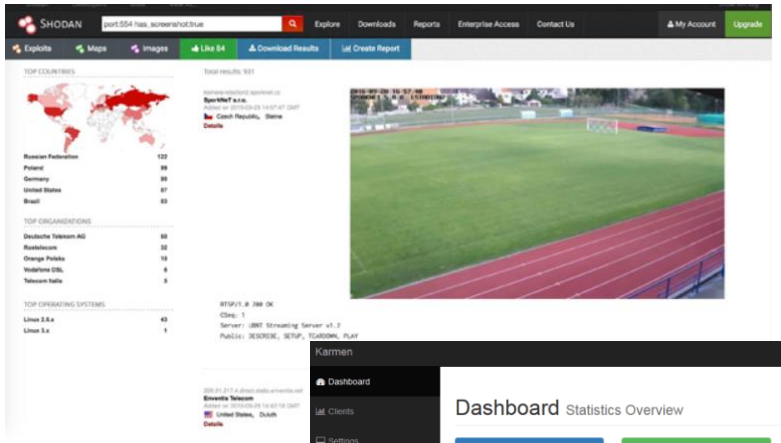
- Expérience de 7 ans dans l‘intégration de solution cybersécurité
- Expert sécurité défensive
- Certifié Fortinet

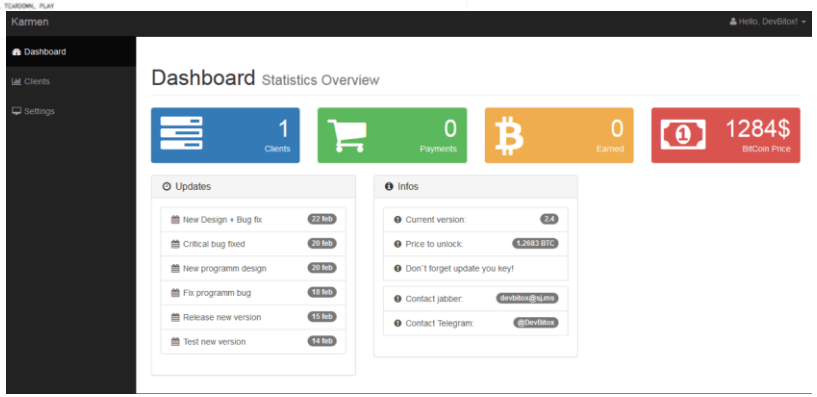
Bechtle BU PS - Réseau et sécurité

Agenda.

1. Contexte
2. Fortinet
3. Protection périmétrique
4. Sécurité interne
5. Visibilité et traçabilité
6. Fortinet Security Fabric

Contexte – Attaquant





- Outils disponibles et démocratisés
- Professionnalisation des attaquants

Contexte – Défense

- Surface d’attaque
- Visibilité
- Automatisation et efficacité opérationnelle
- Compliance

Fortinet – Présentation

- Fondé en 2000 par Ken Xie
- Reconnu comme un leader sur le marché de la sécurité
- Portefeuille complet
- Plus de 480 000 clients
- Service Fortiguard

Source: Gartner (September 2020)

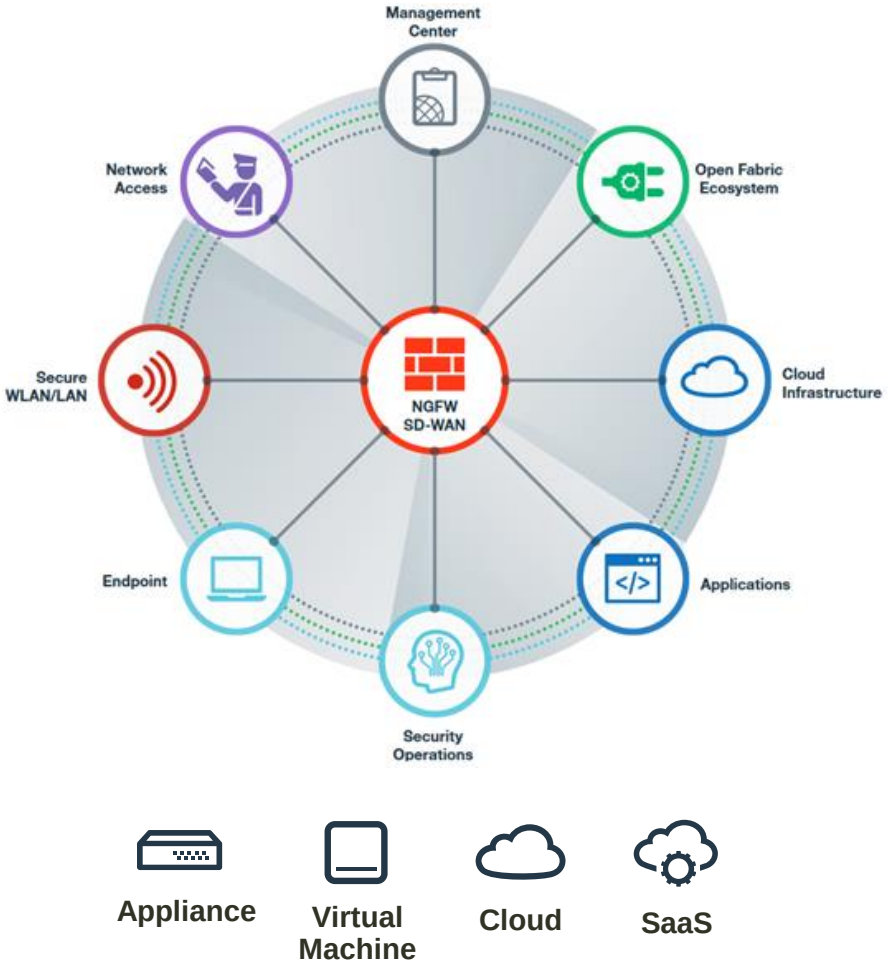
Figure 1. Magic Quadrant for Network Firewalls

Source: Gartner (November 2020)

Fortinet - Security Fabric

Réponse de cyber-protection aux évolutions digitales des entreprises

- Visibilité sur l'infrastructure pour gérer le risque efficacement
- Intégration des solutions Fortinet permettant de réduire les contraintes de support de multiples solutions
- Réponse cohérente et automatisée aux attaques sophistiquées



Fortinet Security Fabric – Use Case

Reconnaissance

Identification des cibles

Récolte d'informations

Exploitation initiale

Exploitation d'une vulnérabilité

Social Engineering

Phishing

C&C persistance

Maintien des accès de l'équipement compromis

Ajout de modules supplémentaires au trojan

Mouvement latéral

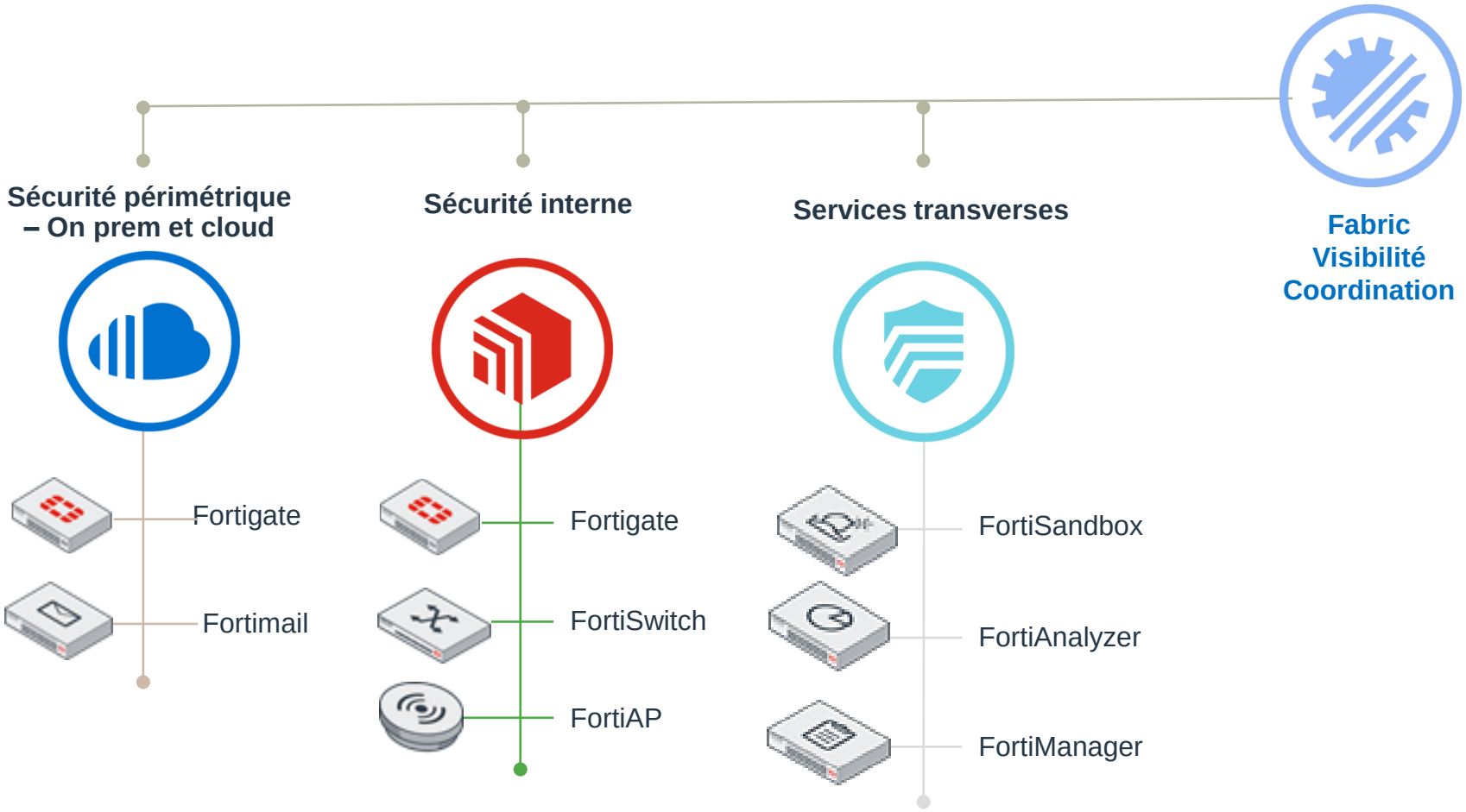
Utilisation de l'équipement/compte piraté pour rebondir dans d'autres zones du système d'information

Exploitaiton finale

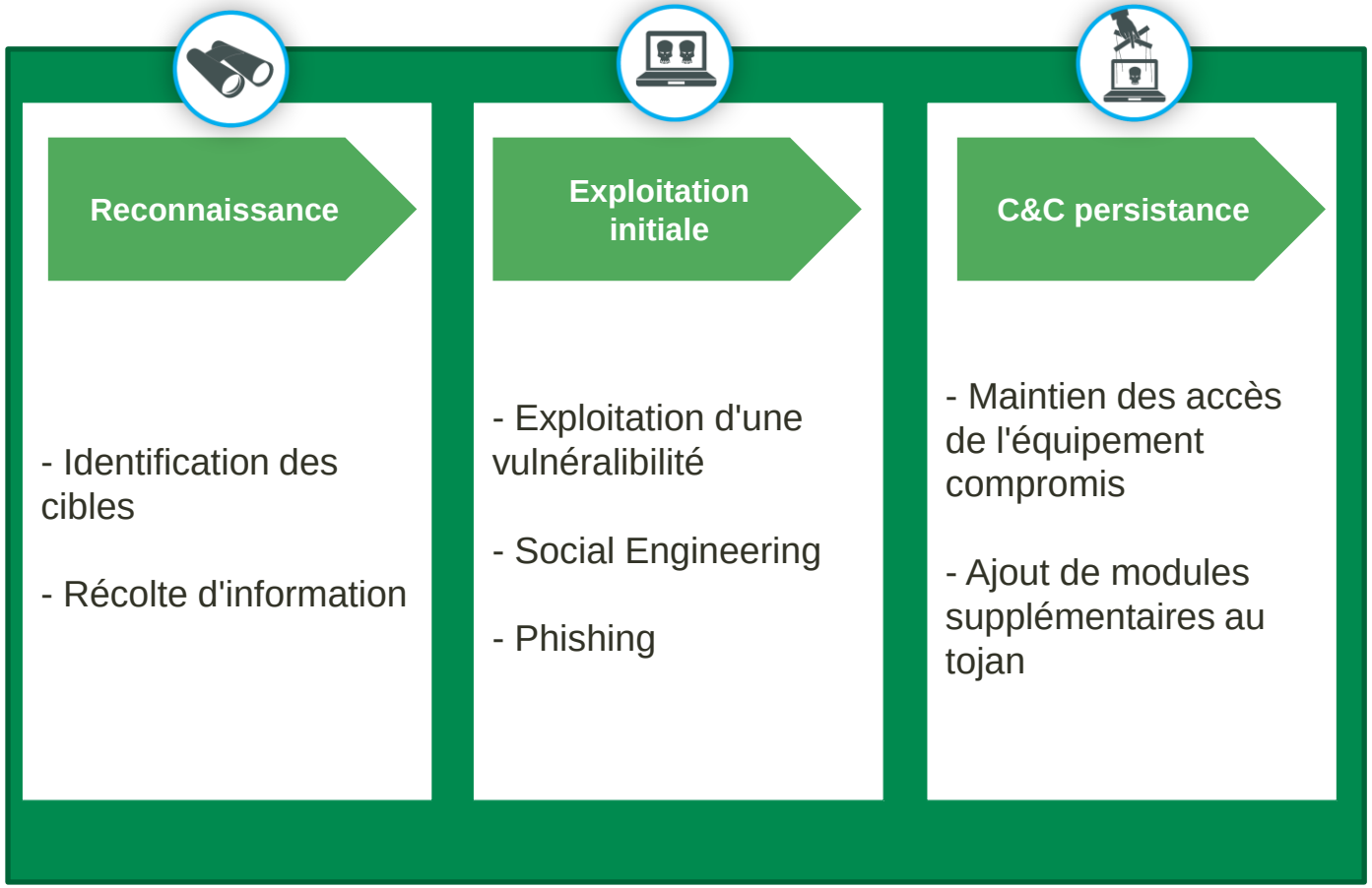
Transfert des informations sensibles en dehors du système d'information de l'entreprise

Chiffrement des données

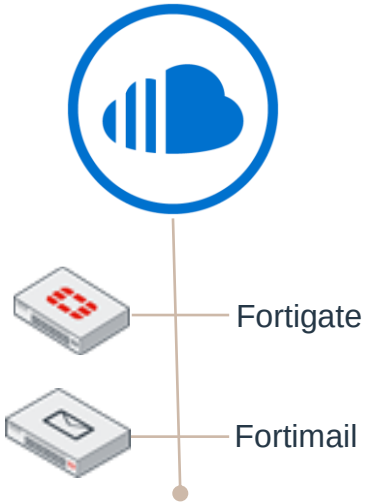
Fortinet Security Fabric – Use Case



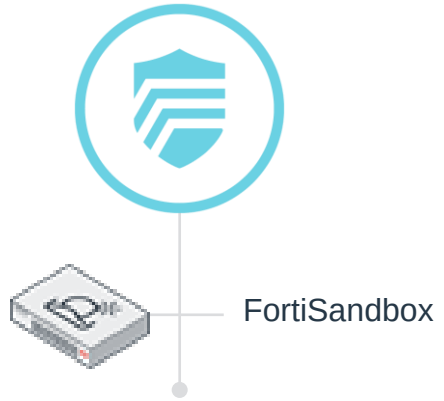
Protection périmétrique



Sécurité périmétrique – On prem et cloud



Services transverses



Protection périmétrique – Vecteurs d'attaque

Emails contenant un document office avec macro malicieuse

PDF Malicieux contenant un exploit adobe

Lien malicieux vers malware

Mail phishing

Mail

Lien malicieux vers téléchargement d'un malware

Faux formulaire

Web

Exploitation d'une vulnérabilité Windows

Exploitation d'une vulnérabilité logicielle

Exploitation frontale

Protection périmétrique - FortiMail

- Certifié et recommandé par différents organismes indépendants
- Multiplateforme
- Intégration O365
- Multiplicité des capteurs de détection

Appliance | Virtual Machine | Cloud | SaaS

ICSA labs CERTIFIED – ADVANCED THREAT DEFENSE – EMAIL

99.9%
Detection of malicious emails across malware types and across malware families.

SE Labs AAA EMAIL SECURITY SERVICES PROTECTION JAN-MAR 2020

94%
Overall Detection Rate

91%
Protection and Legitimate Handling Rate

vb VERIFIED SPAM + virusbtn.com Sept 2020

99.71%
Spam Catch Rate

94.71%
Malware Catch Rate

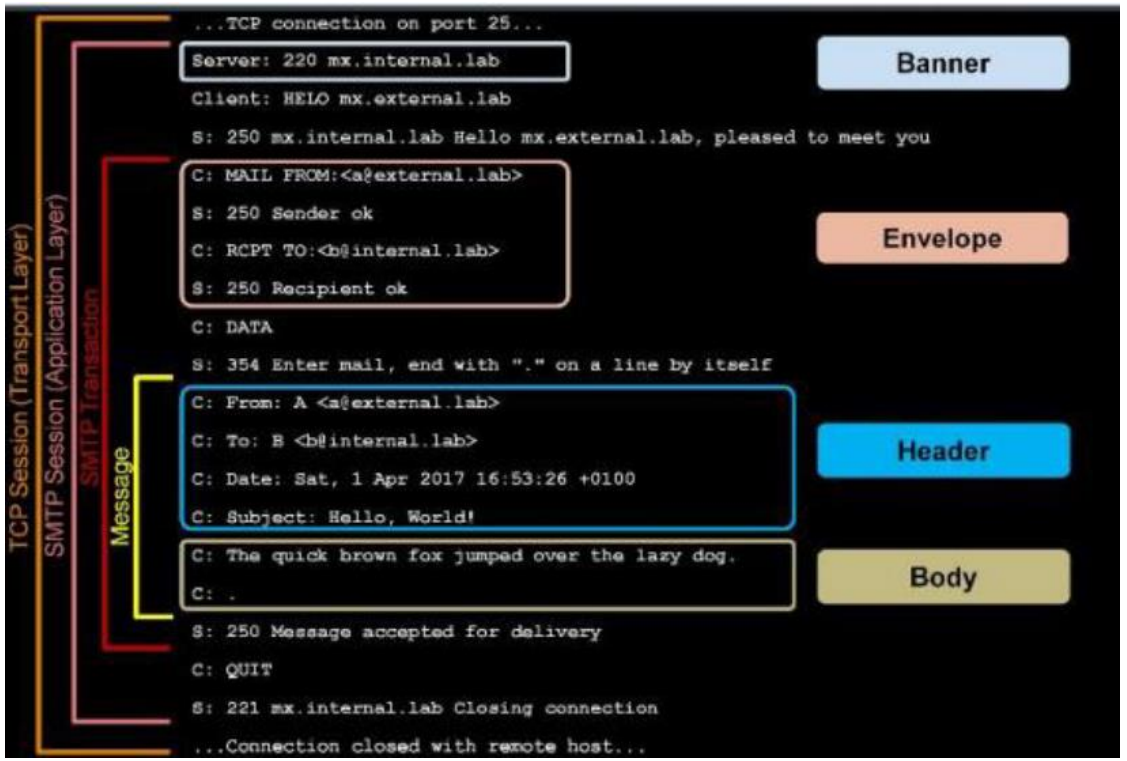
vb 100 VIRUS virusbtn.com

99.5%+
Malware Detection Rate

.01%
False Positive Rate

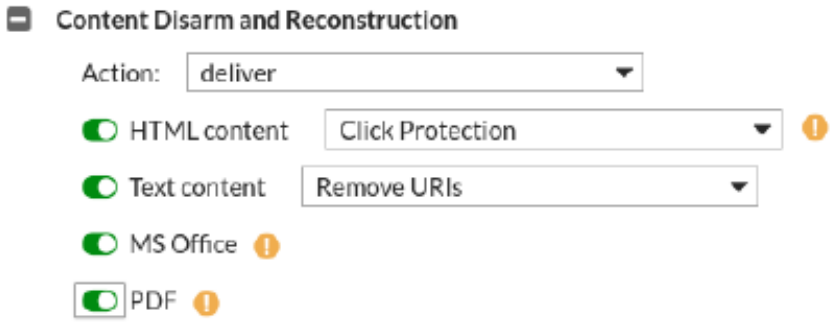
Protection périmétrique - FortiMail

- Protections classiques :
  - SPF / DMARC / DKIM
  - Greylist
  - Fortiguard IP Reputation, Antispam, URL Filtering
  - Filtrage pièce jointe par extension



Protection périmétrique – FortiMail

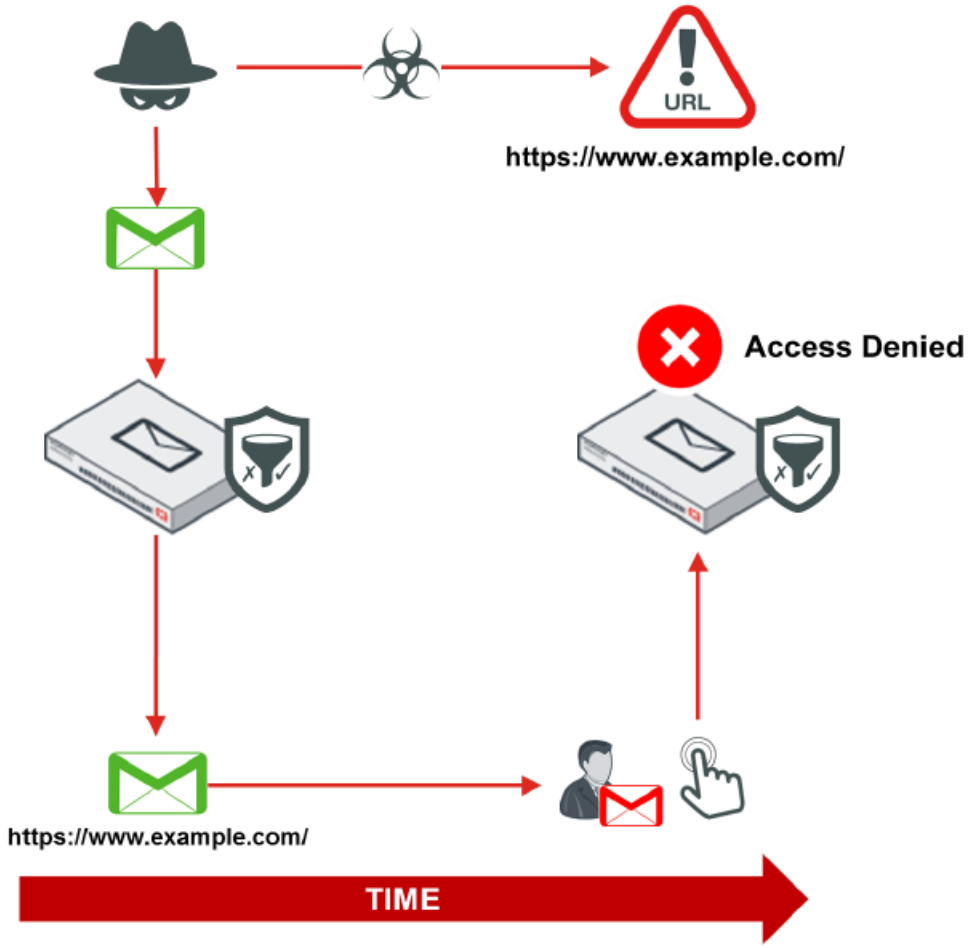
- Content disarm and reconstruction :
  - Enlever le contenu potentiellement dangereux
  - Reconstruction du contenu
  - Transfert du mail




```
...
 office-dde                strip Dynamic Data Exchange fields in Microsoft Office documents
 office-embedded-object    strip embedded objects in Microsoft Office documents
 office-hyperlink          strip hyperlinks in Microsoft Office documents
 office-linked-object      strip linked objects in Microsoft Office documents
 office-macro              strip macros in Microsoft Office documents
 pdf-action-form           strip actions that submit data to other targets in PDF documents
 pdf-action-gotor          strip links to other PDF documents in
...
```

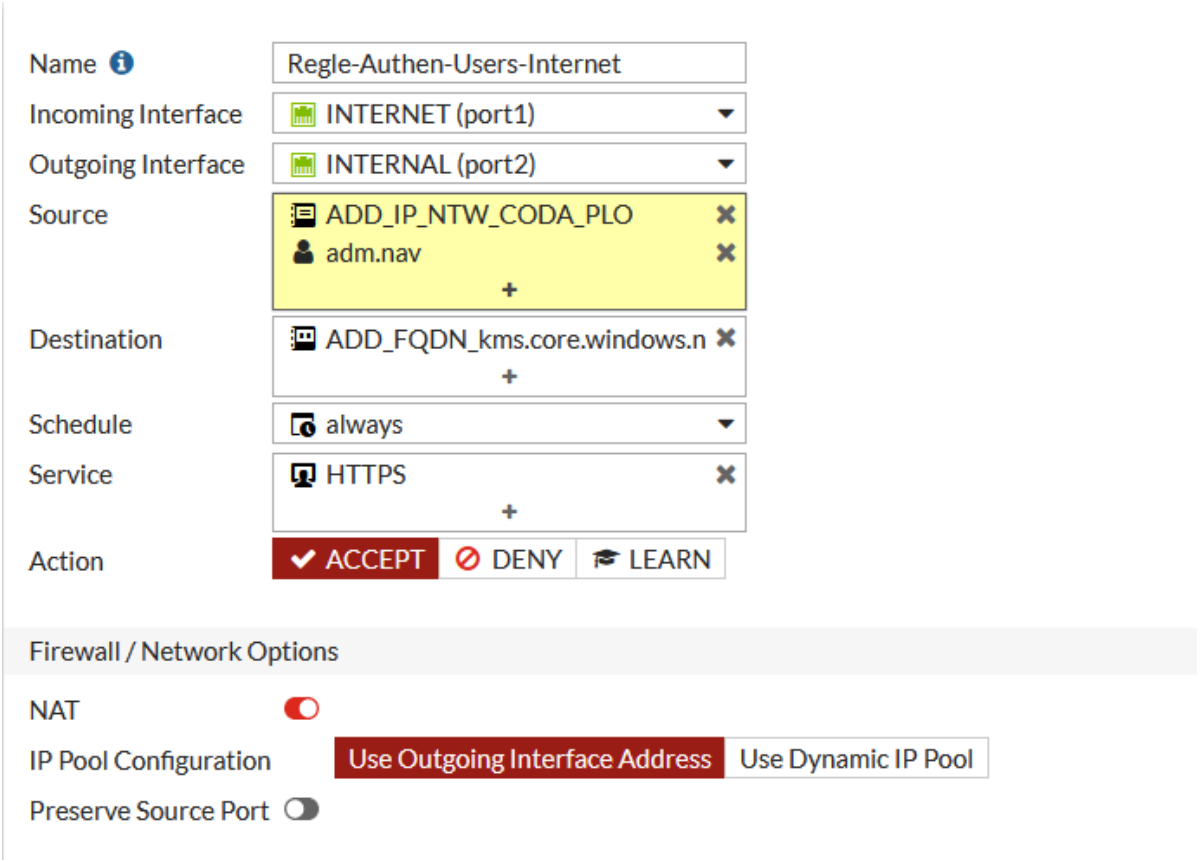
Protection périmétrique – FortiMail

- Outbreak protection
- Click and Protect:
  - URL’s sont réécrites par le Fortimail
  - FortiMail rescanne le lien lorsque l’utilisateur clique dessus
- Transmission Sandboxing



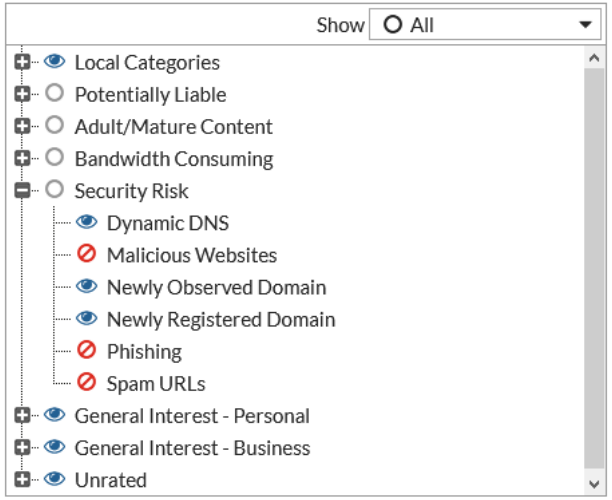
Protection périmétrique – FortiGate

- Next Generation Firewall
- Hardware, VM, Cloud
- FortiOS
- Segmentation réseau et filtrage protocolaire
- Unified Threat Management



Protection périmétrique – FortiGate

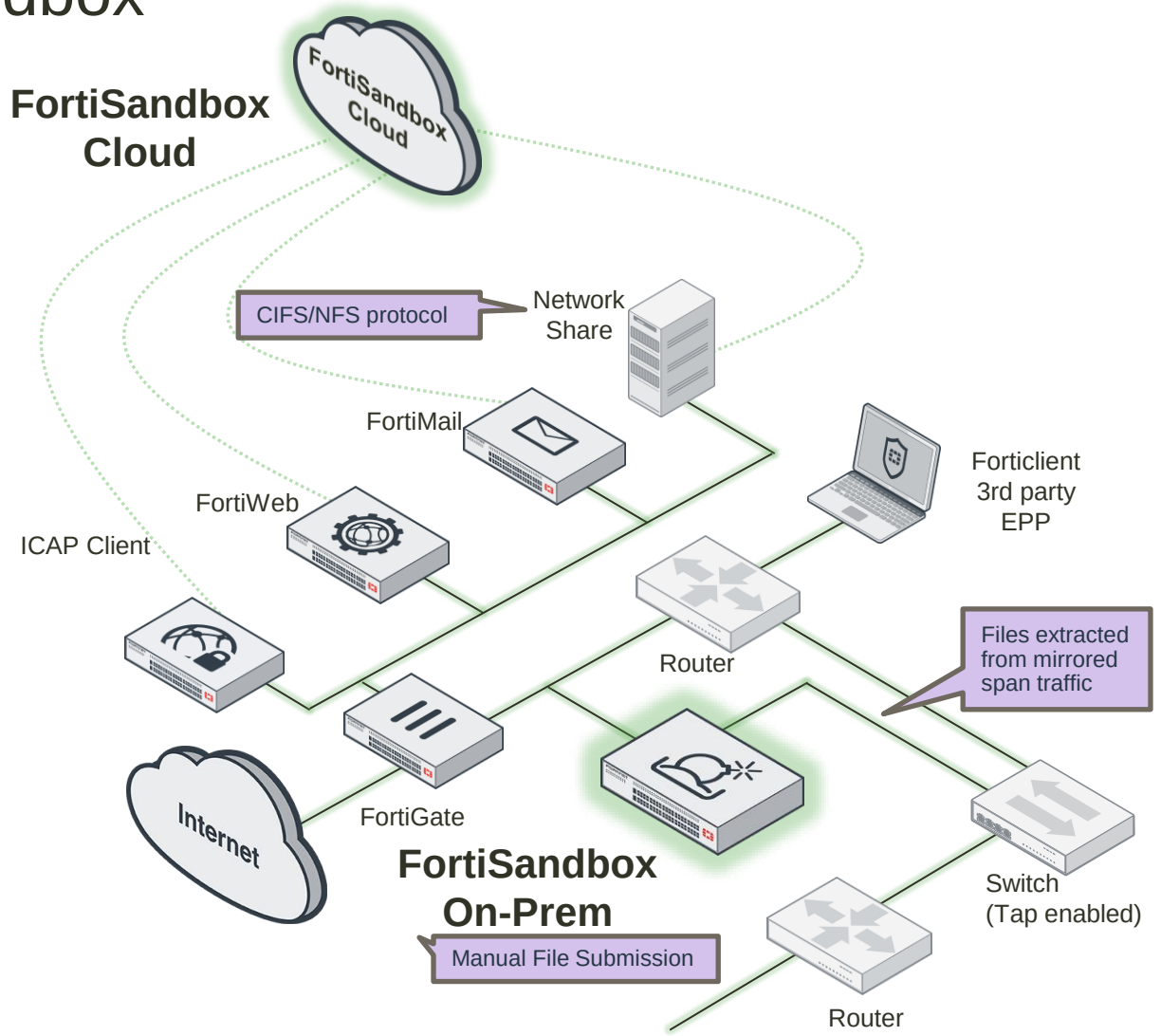
- IPS
- Anti-Virus
- Filtrage Web
- Application control



Name	Category	Technology	Popularity	Risk
ActMobile.VPN	Proxy	Client-Server	★★☆☆☆	
Amaze.VPN	Proxy	Client-Server	★★☆☆☆	
AnonymoX	Proxy	Client-Server	★☆☆☆☆	
AnonyTun	Proxy	Client-Server	★★☆☆☆	
AppVPN	Proxy	Client-Server	★★☆☆☆	
ASProxy	Proxy	Browser-Based	★★★☆☆	
Astrill	Proxy	Client-Server	★★☆☆☆	
Atom.VPN	Proxy	Client-Server	★☆☆☆☆	
AutoHideIP	Proxy	Client-Server	★★☆☆☆	
Avira.Phantom.VPN	Proxy	Client-Server	★★★★☆	
Bestline.VPN	Proxy	Client-Server	★★☆☆☆	
Betternet.VPN	Proxy	Client-Server	★★★★☆	
Blockless.Proxy.VPN	Proxy	Client-Server	★☆☆☆☆	
BlueSurface	Proxy	Client-Server	★★☆☆☆	
Browsec	Proxy	Client-Server	★★★☆☆	
CGIProxy	Proxy	Browser-Based	★☆☆☆☆	
Cisco.VPN.Client	Proxy	Client-Server	★★★★☆	
Cloud.VPN	Proxy	Client-Server	★★★☆☆	
Cloudflare.1.1.1.1.VPN	Proxy	Client-Server	★☆☆☆☆	
Cow.VPN	Proxy	Browser-Based	★★☆☆☆	
CProxy	Proxy	Client-Server	★☆☆☆☆	
Croxy.Proxy.VPN	Proxy	Client-Server	★☆☆☆☆	
CyberGhost.VPN	Proxy	Client-Server	★★★☆☆	

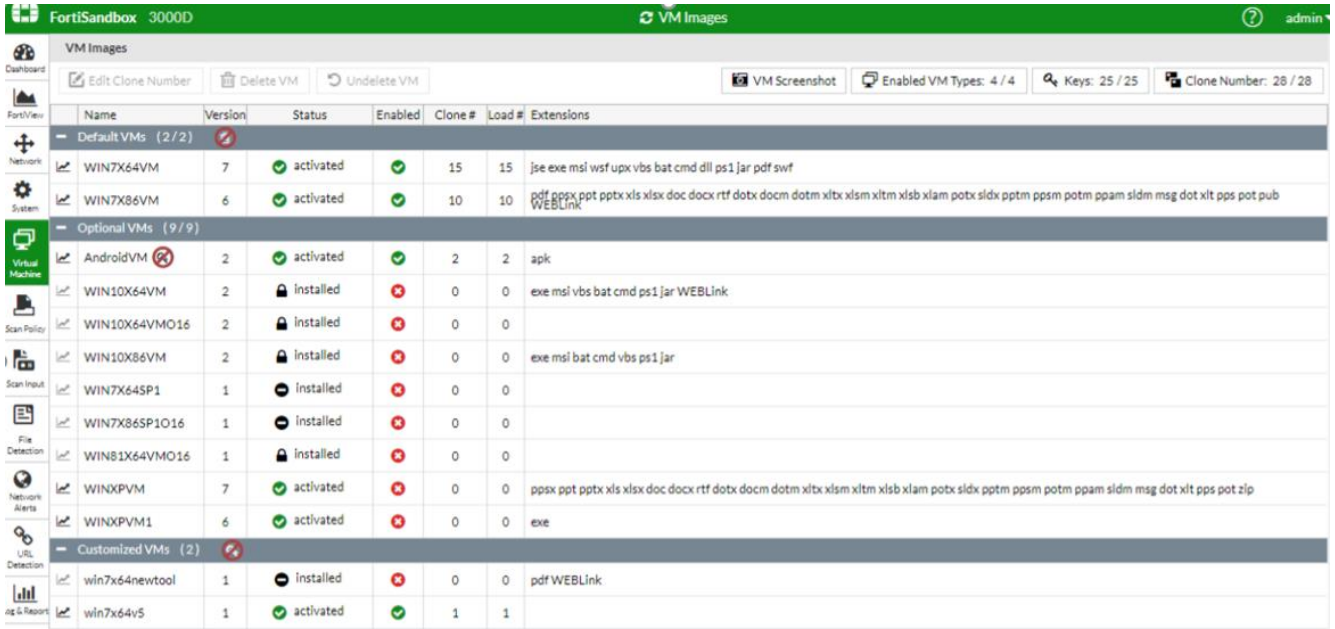
Protection périmétrique – FortiSandbox

- Analyse comportementale fichier/URI dans un environement sécurisé
- Déploiement flexible :
  - Soumission fichier automatique équipements Fortinet
  - Network Share
  - Span traffic
  - ICAP
  - Soumission manuelle
- Création et partage IoC



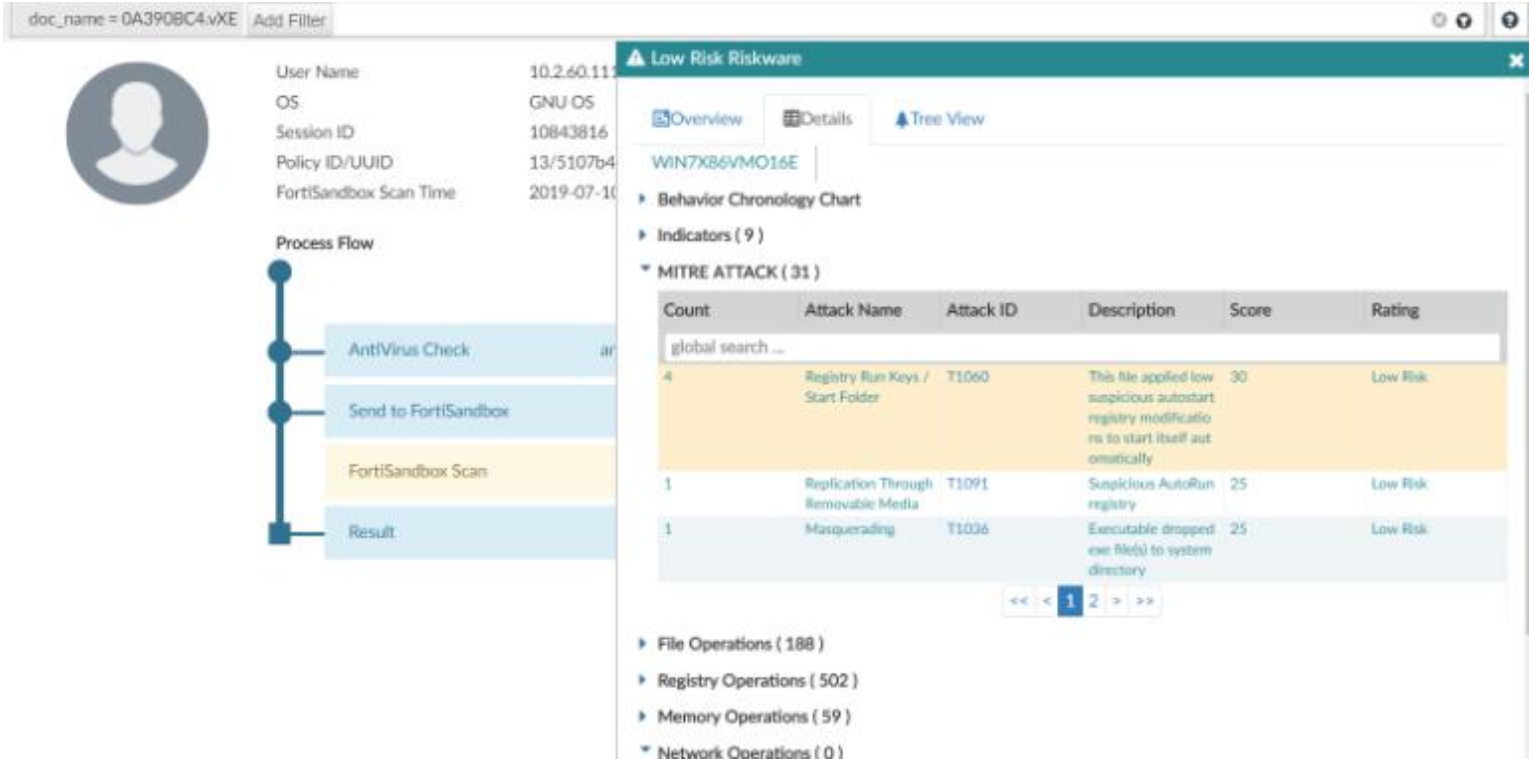
Protection périmétrique – FortiSandbox

- Multi OS
- Possibilité de mettre une VM golden image
- Rapport détaillé

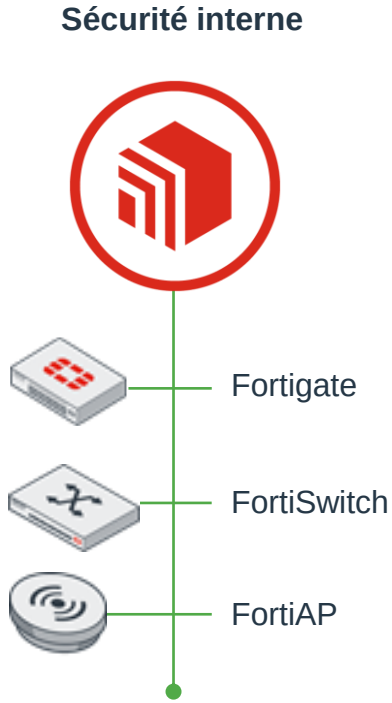


Protection périmétrique – FortiSandbox

- Chronologie action
- Activité complète :
  - Fichiers
  - Mémoire
  - Registre
- Flux réseaux



Protection Interne

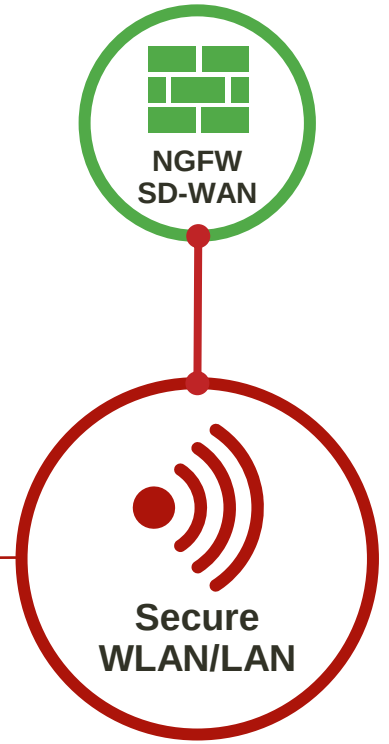


Sécurité interne - Présentation

La couche Access est souvent délaissée et n'est pas intégrée à la sécurité globale de l'infrastructure.

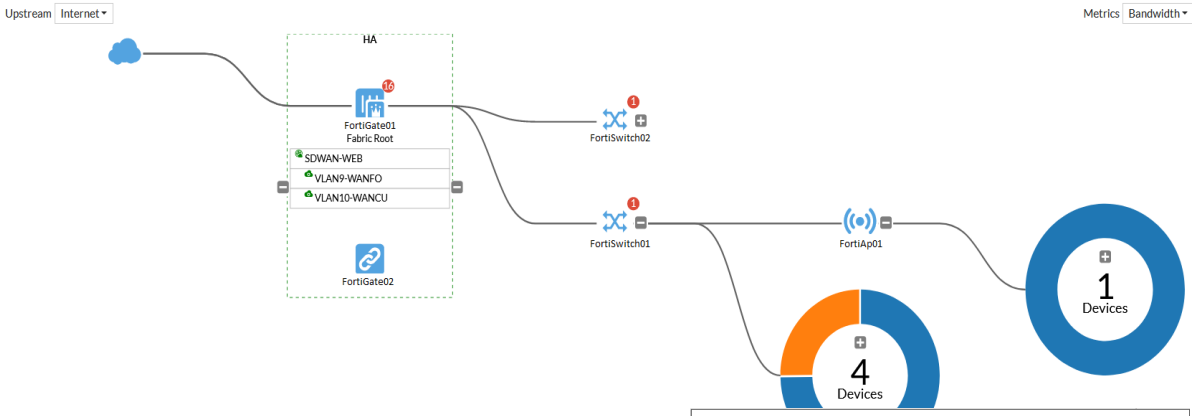
FortiGate **FortiAP** **FortiSwitch**

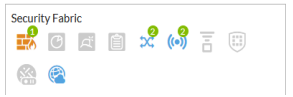
- Etendre la sécurité à la couche access
- Simplifier la gestion

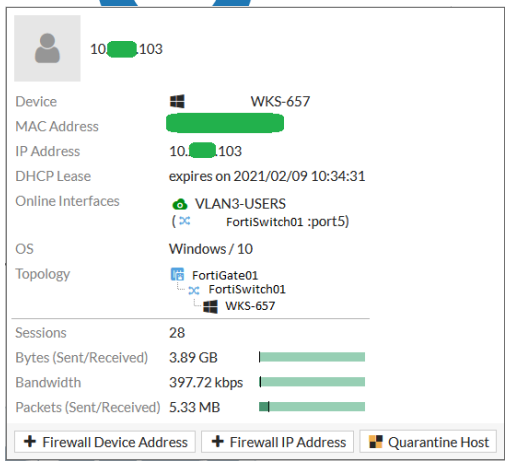


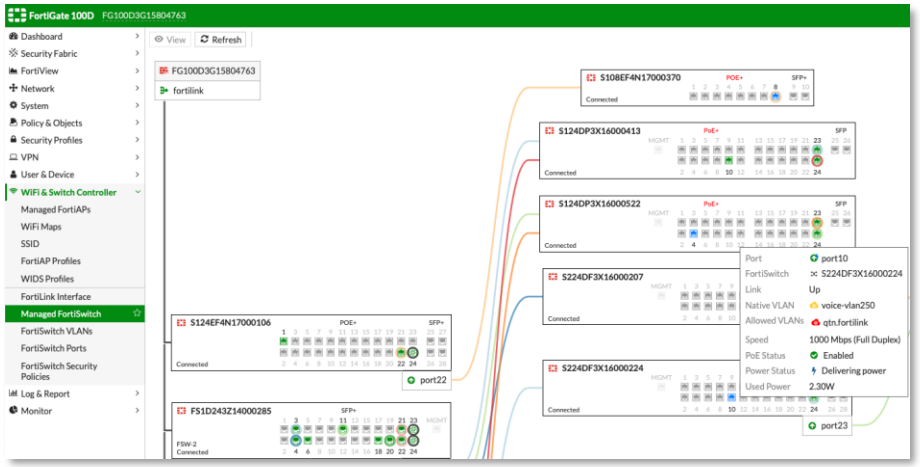
Sécurité interne - Fortiswitch

- Segmentation L2 (802.1Q)
- Intègre toutes les fonctionnalités de sécurité L2 (DHCP snooping, RootGuard, AdminEdge)
- Identification des machines connectées grâce au 802.1X
- Intégration à la Security Fabric
- Management centralisé grâce au FortiLink sur les FortiGate



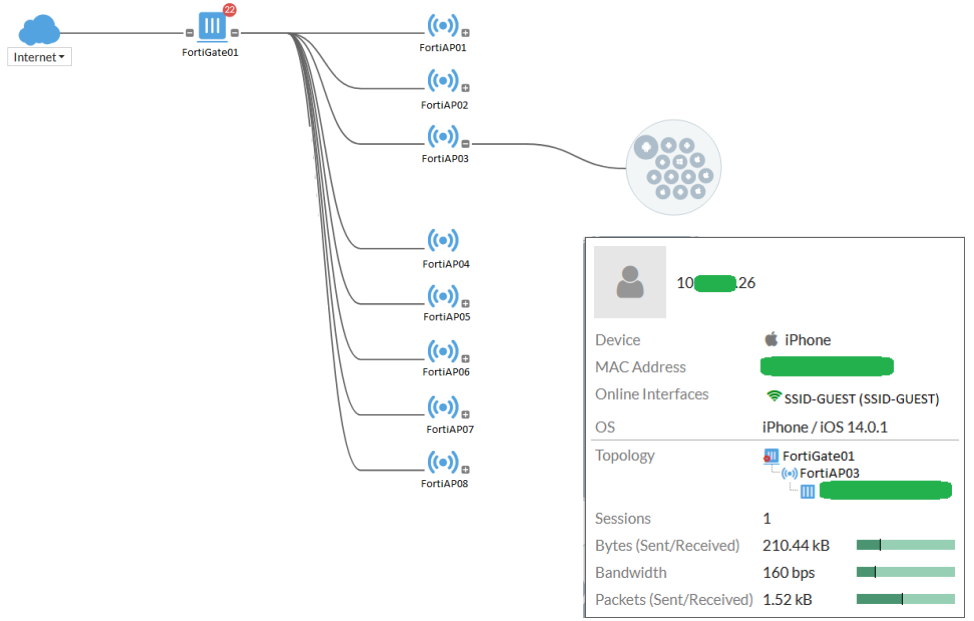


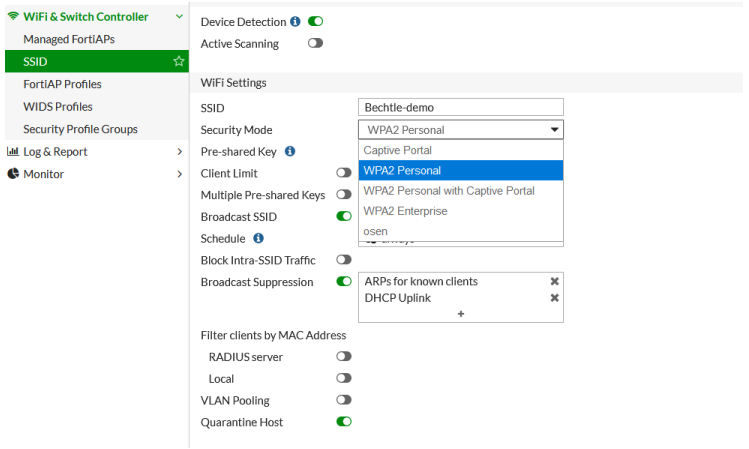




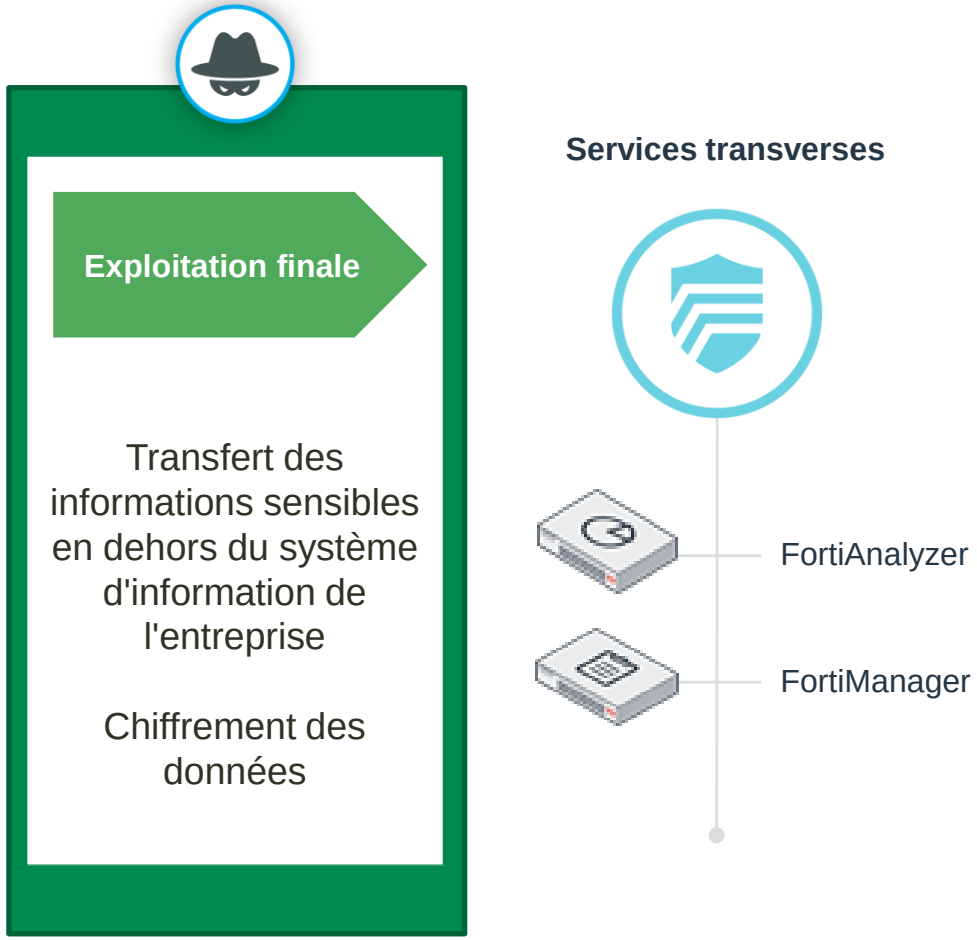
FortiAP

- Contrôleur Wifi intégré au FortiGate
- Isolation des équipements
- Intégration à la Security Fabric
- Facilité de configuration





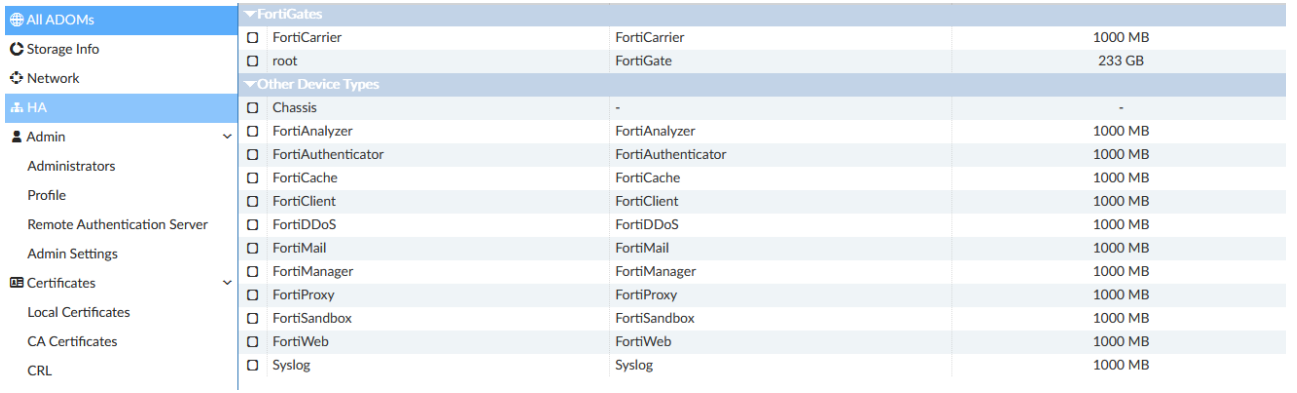
Visibilité et traçabilité



Visibilité - FortiAnalyzer

FortiAnalyzer – Centralisation log

- Multi-Plateforme
- Centralisation log et évènements
- Aggrégation, correlations des logs
- Serveur syslog

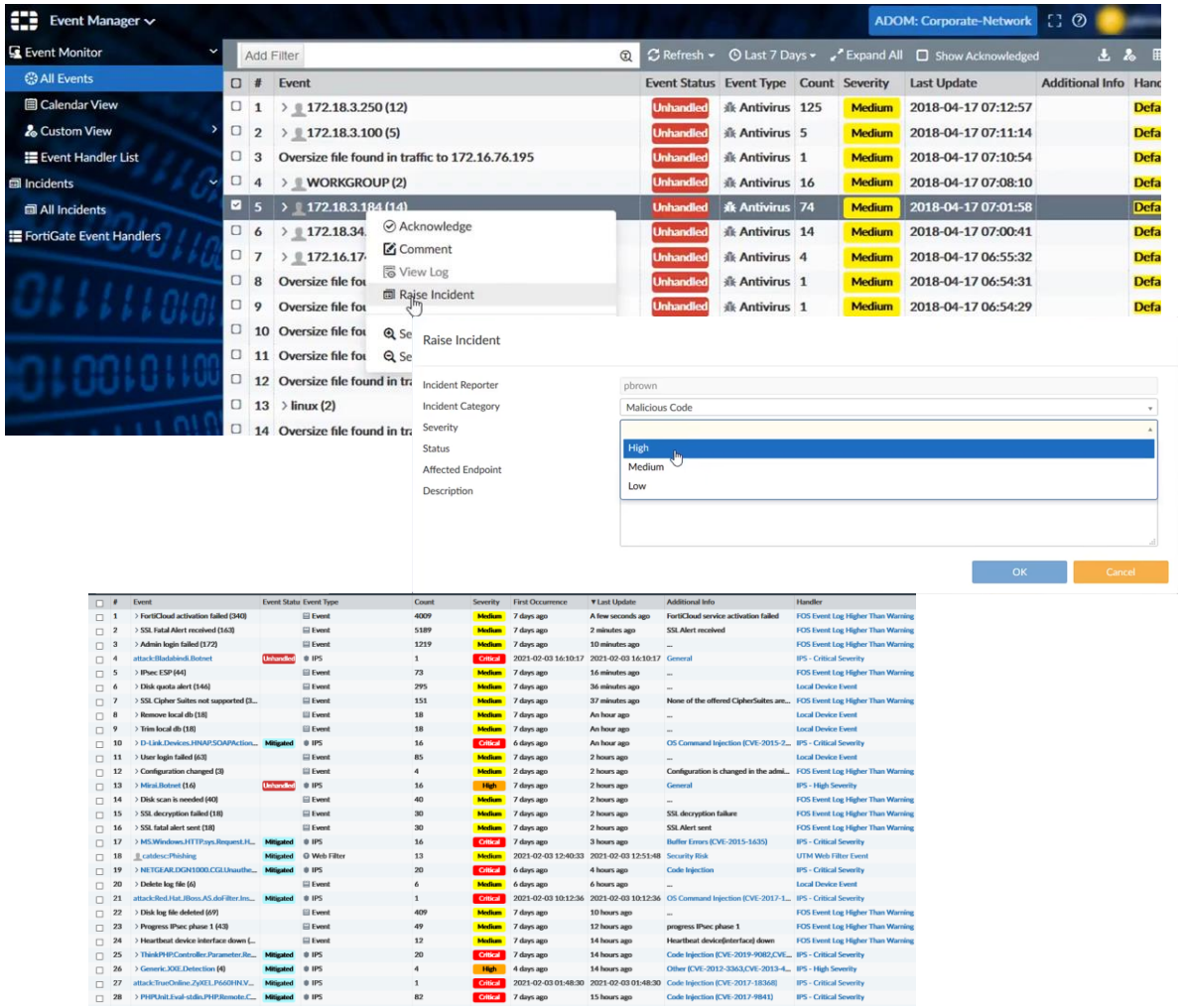


#	Date/Time	Device ID	Severity	Source	Attack Name	Action
1	16:10:17	FGT90D3Z1501	critical	66.240.205.34	Bladabindi.Botnet	dropped
2	15:58:36	FGT90D3Z1501	low	199.19.226.67	ZmEu.Vulnerability.Scanner	dropped
3	15:58:31	FGT90D3Z1501	low	199.19.226.67	ZmEu.Vulnerability.Scanner	dropped
4	14:55:33	FG100D3G1582	critical	120.85.92.135	D-Link.Devices.HNAP.SOAPAction-Header.Command...	dropped
5	14:14:51	FG100D3G1582	high	103.82.144.197	Mirai.Botnet	dropped
6	13:53:41	FGT90D3Z1501	critical	66.240.205.34	MS.Windows.HTTP.sys.Request.Handling.Remote.Cod...	dropped
7	12:00:02	FGT90D3Z1501	critical	221.15.239.47	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.C...	dropped
8	10:59:14	FG100D3G1582	low	199.19.226.67	ZmEu.Vulnerability.Scanner	dropped
9	10:59:08	FG100D3G1582	low	199.19.226.67	ZmEu.Vulnerability.Scanner	dropped
10	10:12:36	FGT90D3Z1501	critical	197.3.8.66	Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization	dropped
11	09:09:51	FGT90D3Z1501	low	142.93.123.76	Mublackcat.Scanner	dropped
12	09:09:51	FGT90D3Z1501	low	142.93.123.76	Mublackcat.Scanner	dropped
13	09:09:46	FGT90D3Z1501	low	142.93.123.76	Mublackcat.Scanner	dropped
14	09:09:46	FGT90D3Z1501	low	142.93.123.76	Mublackcat.Scanner	dropped
15	09:09:41	FGT90D3Z1501	low	142.93.123.76	Mublackcat.Scanner	dropped
16	09:09:36	FGT90D3Z1501	low	142.93.123.76	Mublackcat.Scanner	dropped
17	06:31:26	FGT90D3Z1501	critical	93.124.15.205	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.C...	dropped
18	05:16:05	FGT90D3Z1501	critical	27.41.6.234	D-Link.Devices.HNAP.SOAPAction-Header.Command...	dropped
19	03:04:00	FGT90D3Z1501	high	221.178.127.128	Mirai.Botnet	dropped
20	01:55:55	FGT90D3Z1501	critical	45.155.205.108	ThinkPHP.Controller.Parameter.Remote.Code.Execution	dropped
21	01:55:55	FGT90D3Z1501	high	45.155.205.108	Generic.XXE.Detection	dropped
22	01:48:30	FGT90D3Z1501	critical	172.98.64.135	TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Com...	dropped
23	01:27:30	FGT90D3Z1501	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped
24	01:27:30	FGT90D3Z1501	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped
25	01:26:15	FGT90D3Z1501	critical	66.240.205.34	GhOst.Rat.Botnet	dropped
26	02-02 23:21	FG100D3G1582	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped
27	02-02 23:21	FG100D3G1582	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped
28	02-02 23:19	FG100D3G1582	high	45.155.205.108	Generic.XXE.Detection	dropped
29	02-02 23:19	FG100D3G1582	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped
30	02-02 23:07	FGT90D3Z1501	medium	45.155.205.108	PHP.Diescan	dropped
31	02-02 23:07	FGT90D3Z1501	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped

Visibilité - FortiAnalyzer

FortiAnalyzer – Réponse à incident

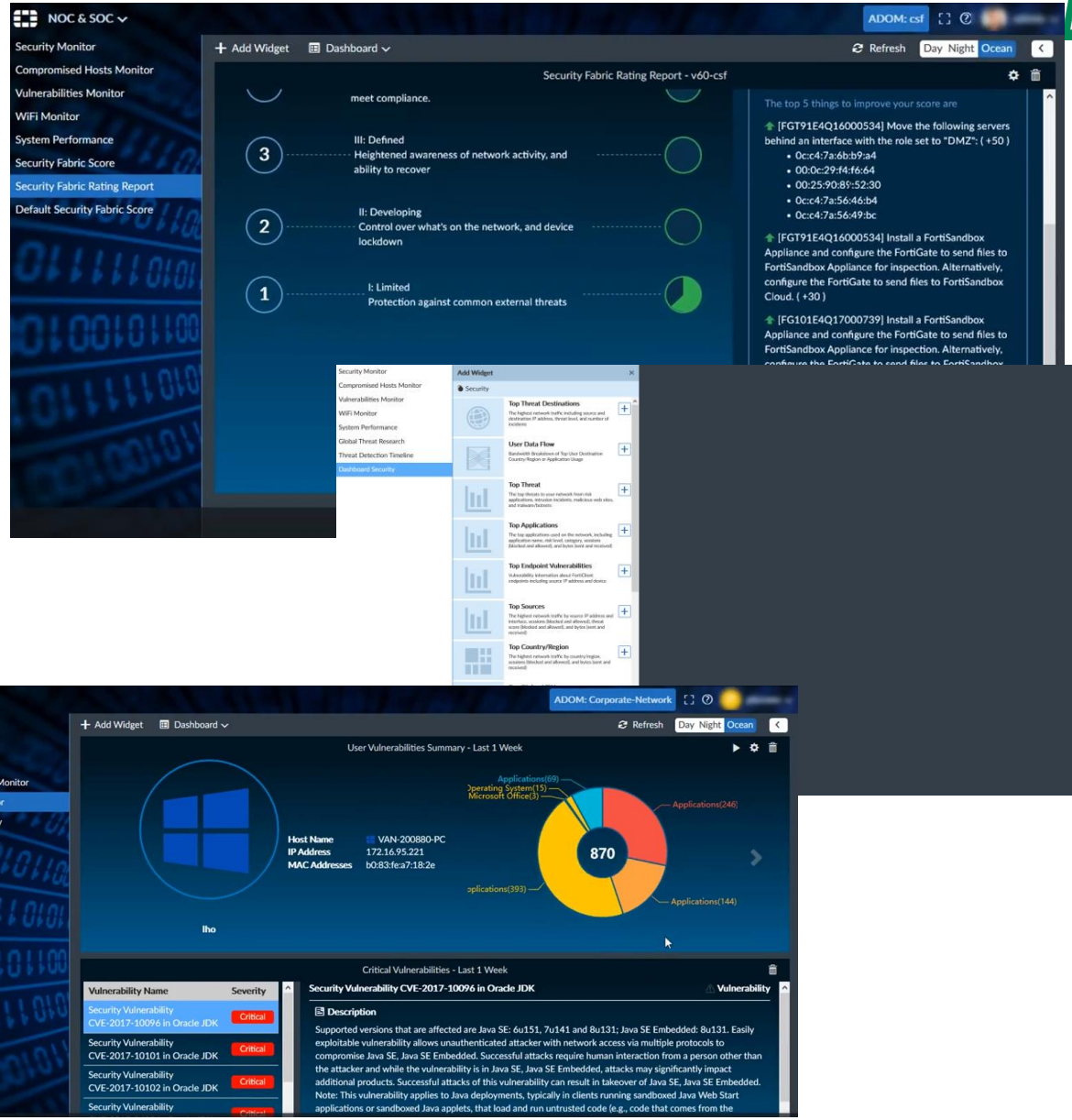
- Event Manager
- Connectivité possible avec les ITSM déja en place (ServiceNow)



Visibilité - FortiAnalyzer

FortiAnalyzer – SOC & NOC

- Fonctionnalité Noc / Soc permet d'avoir un état des lieux de votre infrastructure
  - Une visibilité complète grâce à la centralisation des logs
  - Des widgets personnalisables
- Security Fabric rating / Security fabric Score
- Vulnerabilities Monitor :
  - Une visibilité accrue sur l'état sécuritaire des machines.
  - Des remédiations sur les vulnérabilités détectées



Visibilité - FortiAnalyzer

FortiAnalyzer - Rapport

- Modèles de rapport pour tout type de population :
  - Board
  - Equipe Technique
- Personnalisation des rapports
- Génération du rapport planifiée

Top 20 Most Blocked Categories

#	Category	Requests
1	Instant Messaging	46,310
2	Streaming Media and Download	5,583
3	Social Networking	2,288
4	File Sharing and Storage	689
5	Pornography	42
6	Web Chat	22
7	Gambling	10
8	Newly Observed Domain	6
9	Games	6
10	Unrated	4
11	Web-based Email	4
12	Freeware and Software Downloads	4
13	Malicious Websites	2
14	Alcohol	2
15	Dating	2
16	Newly Registered Domain	1

Botnet Detected

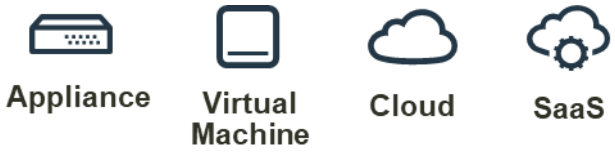
#	Botnet Name	Counts
1	Mirai.Botnet	17
2	Gh0st.Rat.Botnet	1

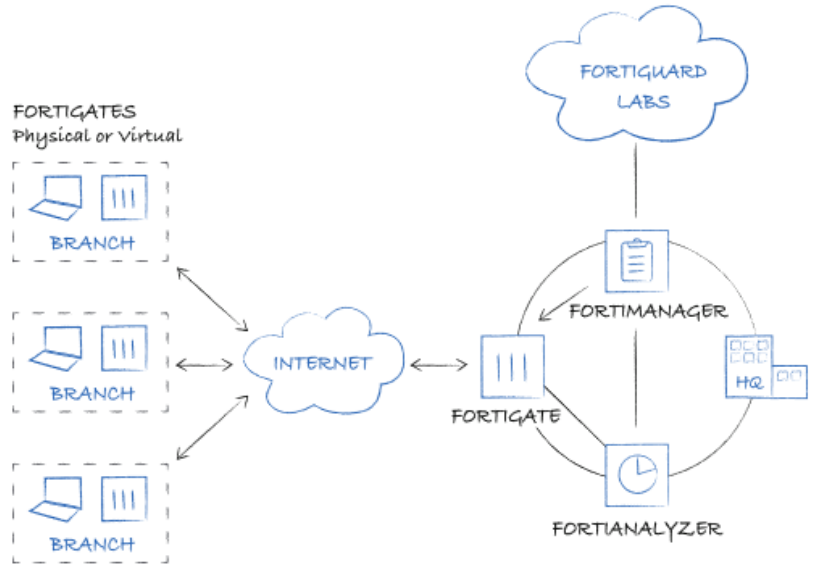
Intrusions Detected

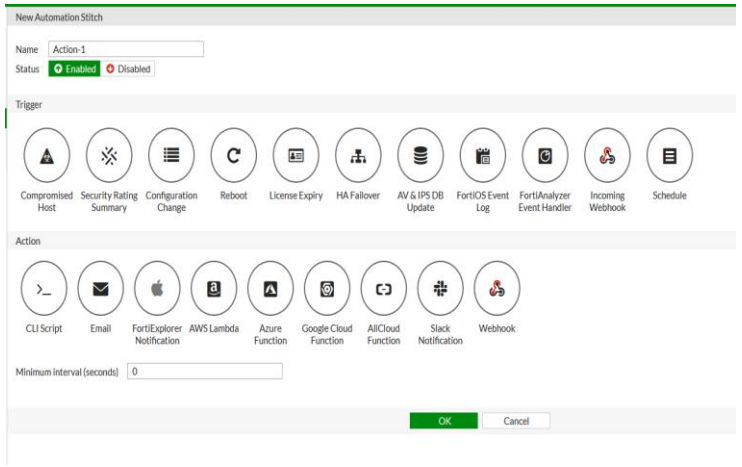
#	Attack Name	Severity	CVE-ID	Counts
1	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Critical	CVE-2017-9841	86
2	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	Critical	CVE-2019-16759	27
3	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Critical		22
4	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Critical	CVE-2019-9082,CVE-2018-20062	20
5	Dasan.GPON.Remote.Code.Execution	Critical	CVE-2018-10561,CVE-2018-10562	18
6	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	Critical	CVE-2020-7373,CVE-2020-17496	15
7	MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution	Critical	CVE-2015-1635	15
8	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	Critical	CVE-2015-2051,CVE-2019-10891	15
9	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Critical	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	6
10	Apache.Struts.2.REST.Plugin.Remote.Code.Execution	Critical	CVE-2016-4438,CVE-2017-12611	6

Management centralisé - FortiManager

- Multi-Plateforme
- Management centralisé :
  - Règles de filtrage et bases d'objets communes
  - Mises à jour des équipements
  - Sauvegardes des équipements
- Workflow / Orchestration
  - Automatisation

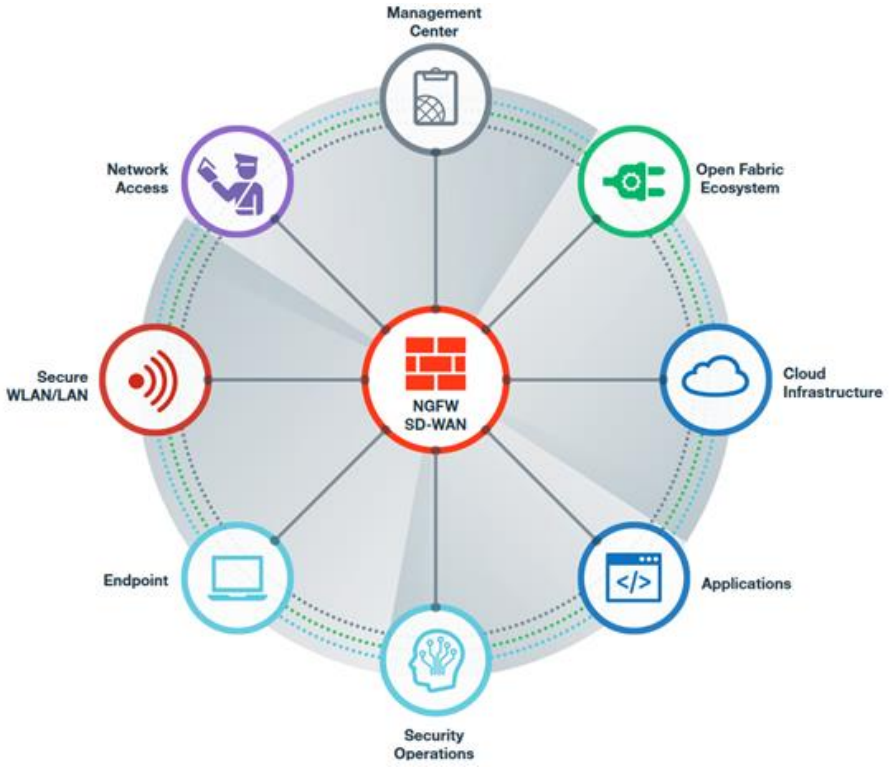






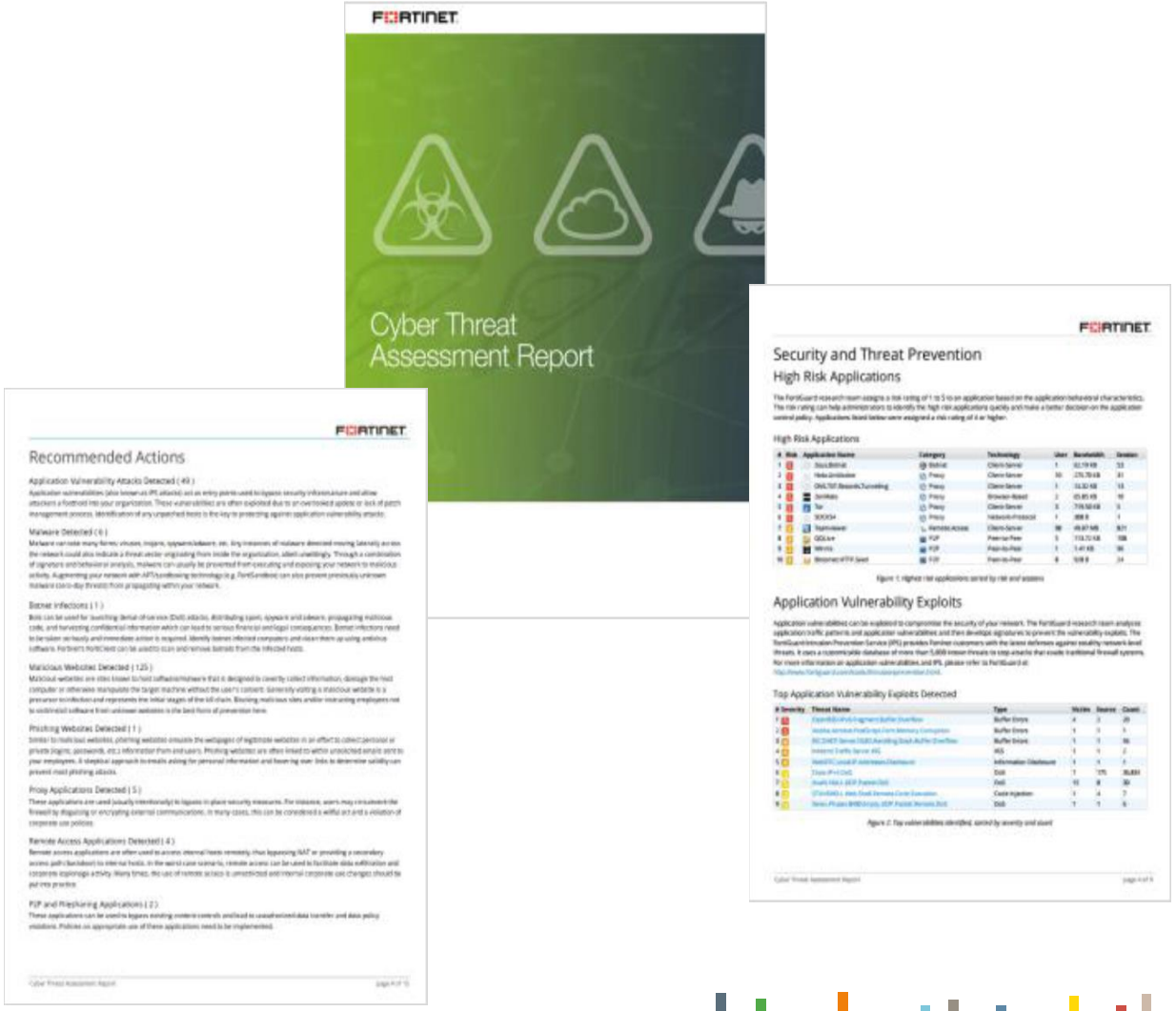
Conclusion

- Fortinet Security Fabric
  - Sécurité en profondeur
  - Optimisation coûts opérationnels et matériel
  - Automatisation
  - Règles de conformité

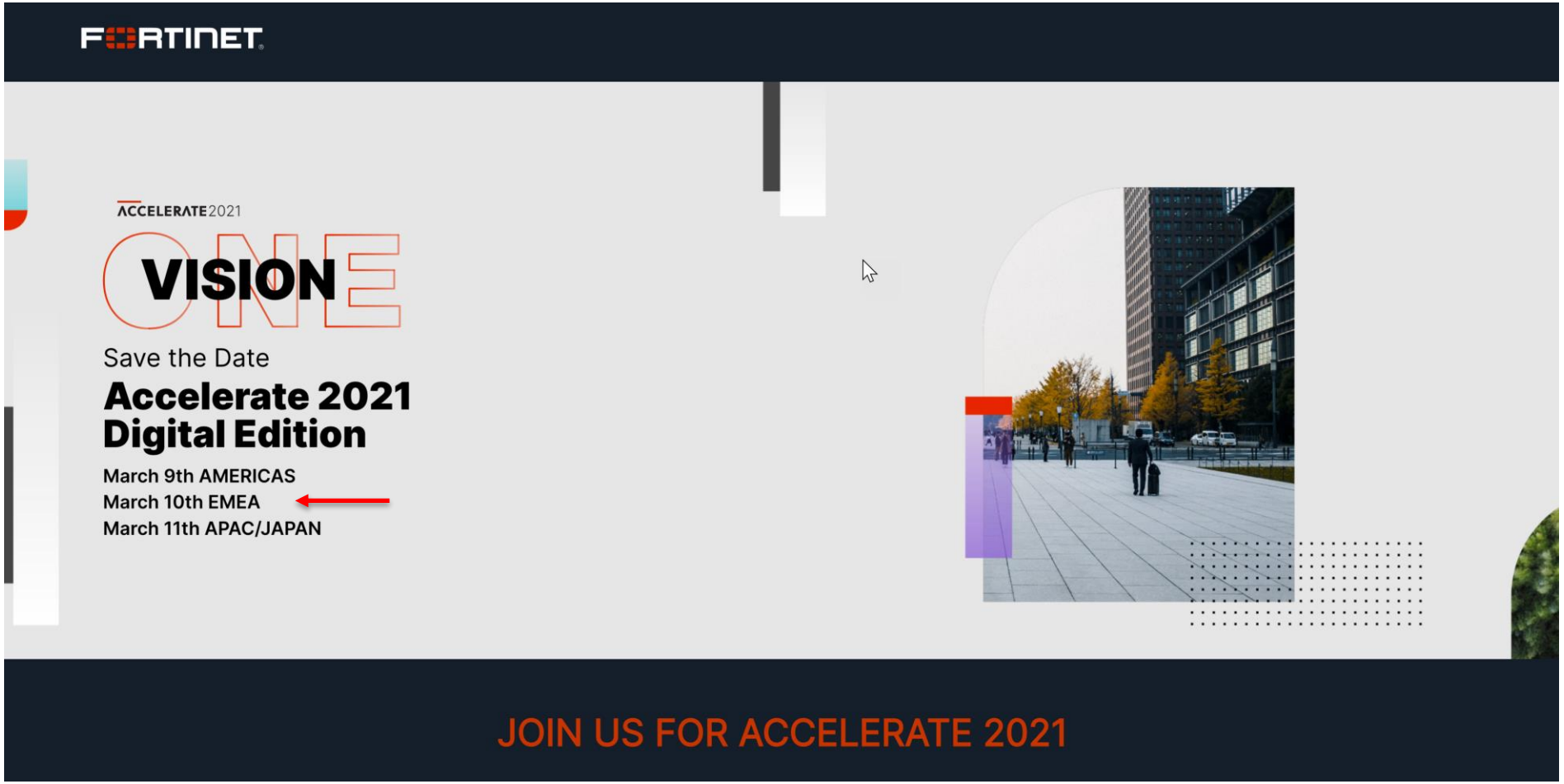


Pour aller plus loin – Fortinet CTAP (Cyber Threat Assessment Program)

- Evalution de l’infrastructure actuelle
- Suite à cette évaluation, un rapport sera établi :
  - Détection potentielle de menaces
  - Analyse du traffic applicatif
  - Des recommandations
- Réseau et mail



Accelerate 2021 EMEA Digital Edition - March 10, 2021



Any questions?

chithavong.chokbengboun@bechtle.com
sylvain.pionchon@bechtle.com

Learn more at
bechtle.com