



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



Bechtel 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

The image shows two screenshots. The top one is a SHODAN search results page for 'port:554 has:screen:0:True'. It displays a world map with search results by country (Russia: 127, Poland: 99, Germany: 87, Brazil: 85) and top organizations (Deutsche Telekom AG: 88, Facebook: 58, Orange Polska: 16, Telekom O2: 8, Telekom Italia: 5). The bottom screenshot is a dashboard for 'Karmen' with statistics: 1 Client, 0 Payments, 0 Earned, and a Bitcoin price of 1284\$. It also shows updates and info sections.

Oday Today Exploit Market and Oday Exploits Database

DESCRIPTION	TYPE	HITS	RISK	GOLD	AUTHOR
Twitter reset account Private Method Oday Exploit	tricks	31,808	██████████	0.196	Oday Today Team
Instagram bypass Access Account Private Method Exploit	tricks	41,170	██████████	0.171	smokzz
SMF 2.1 Beta 2 Remote Code Execution Oday Exploit	php	9,146	██████████	0.298	Protocol8
SMF 2.0.x Remote Code Execution Oday Exploit	php	24,823	██████████	0.426	Protocol8
iCloud reset mail Account Authentication Elevation Of Privilege Oday Exploit	tricks	1,812	██████████	0.384	Oday Today Team
Apple iOS 11.1.1 kernel DoS Exploit	iOS	2,412	██████████	0.426	mashbar
INTERMEDIA CONSOLE - Remote Code Execution Exploit	php	1,798	██████████	0.013	se-az1337
Windows 10 RCE (SandBox Escape/Bypass ASLR/Bypass DEP) Oday Exploit	windows	7,385	██████████	0.512	Oday Today Team

DESCRIPTION	TYPE	HITS	RISK	GOLD	AUTHOR
ALLMediaServer 8.95 - Buffer Overflow Exploit	windows	81	██████████	Free	Mario Kartone
Lab41 wfsAse 3.7 FTP Client - Stack Buffer Overflow Exploit	windows	81	██████████	Free	metasploit
phpCollab 2.5.1 - Unauthenticated File Upload Exploit	php	87	██████████	Free	metasploit
HPD INC ibasec RestAPI Unauthenticated Remote Command Execution Exploit	windows	108	██████████	Free	metasploit
HPD INC ibasec RestAPI Unauthenticated Remote Command Execution Exploit	windows	108	██████████	Free	metasploit
Redbox Enterprise 8.8.18 - Buffer Overflow Exploit	windows	135	██████████	Free	Arin Heijnen
Yazcam 8.6.8 Directory Traversal Vulnerability	windows	111	██████████	Free	David Paster
Comcast Communications Service (cvs) - Command Injection Exploit	windows	159	██████████	Free	metasploit

DESCRIPTION	TYPE	HITS	RISK	GOLD	AUTHOR
Python smtpd 3.7.11 / 3.4.4 / 3.5.1 - Has In The Middle STARTTLS Stripping Vulnerability	multiple	72	██████████	Free	IsInnweb
Firefox Browser < 1.8.18 - Bypass Same Origin Policy Vulnerability	multiple	88	██████████	Free	IsInnweb
Jango Windows 12.3.1 - Privilege Escalation Exploit	windows	98	██████████	Free	Fiber InfoSecurity
Microsoft Windows - Local XPS Print Spooler SandBox Escape Exploit	windows	263	██████████	Free	Google Security
VMware Workstation - ALSA Config File Local Privilege Escalation Exploit	linux	338	██████████	Free	metasploit
Kingsoft Antivirus / Internet Security 9+ - Privilege Escalation Exploit	windows	209	██████████	Free	se-se
Linux Kernel < 4.4.0-83 / < 4.8.0-38 (Ubuntu 14.04/16.04) - Privilege Escalation Exploit	linux	831	██████████	Free	Andrey Konovalov
HP Insight Control For VMware vCenter Server 7.3 Insecure Permissions Vulnerability	windows	209	██████████	Free	GlaKos

- 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

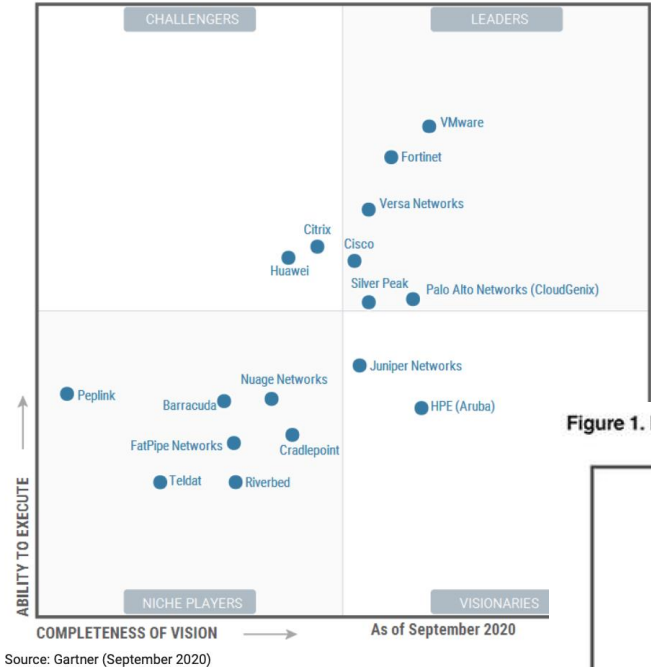


Figure 1. Magic Quadrant for Network Firewalls

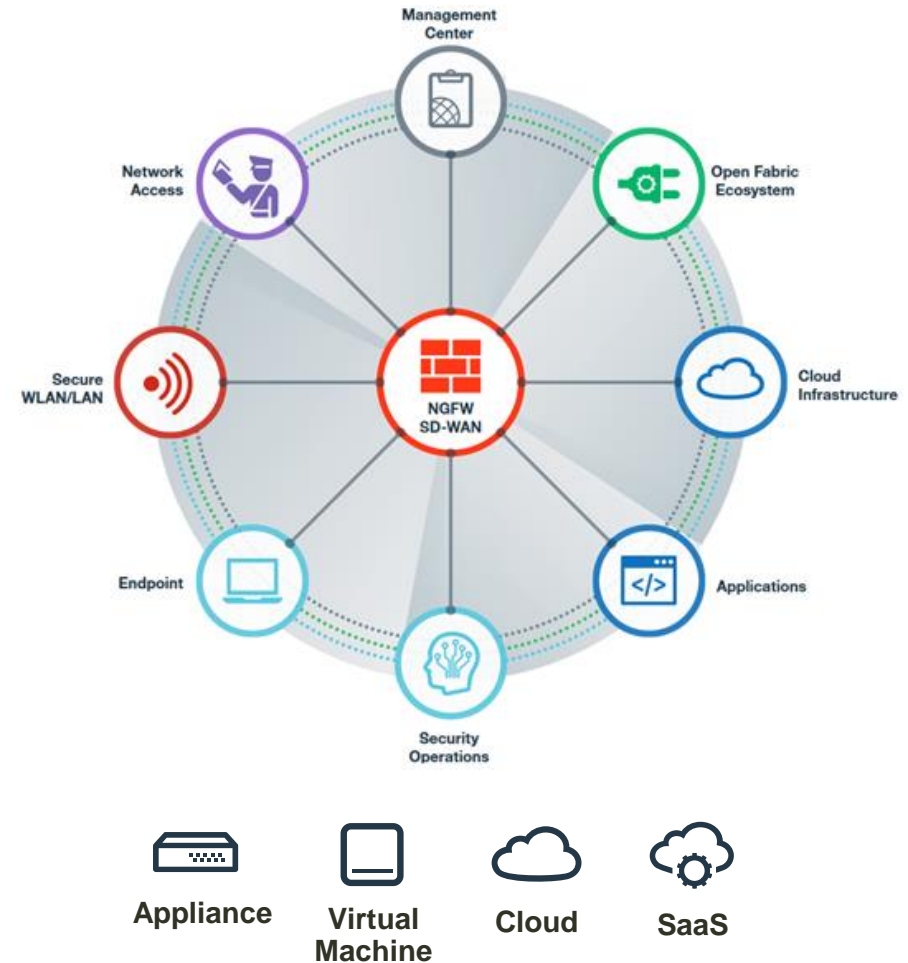


Source: Gartner (November 2020)

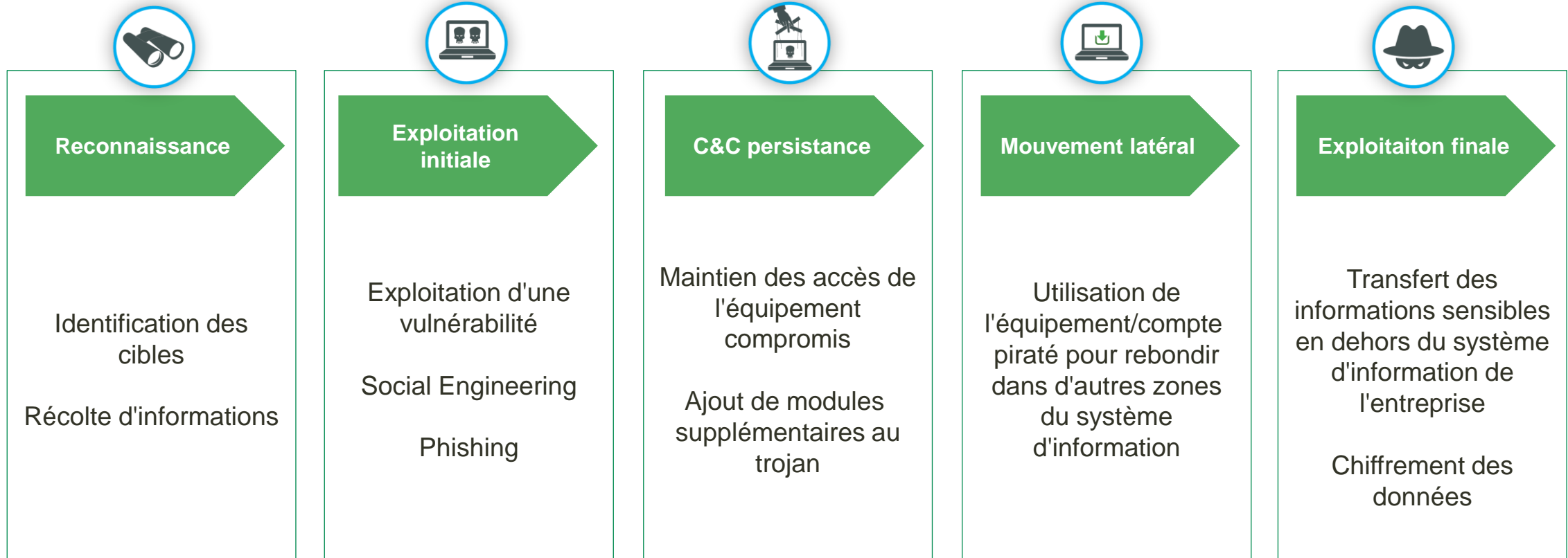
Fortinet - Security Fabric

Réponse de cyber-protection aux évolutions digitales des entreprises

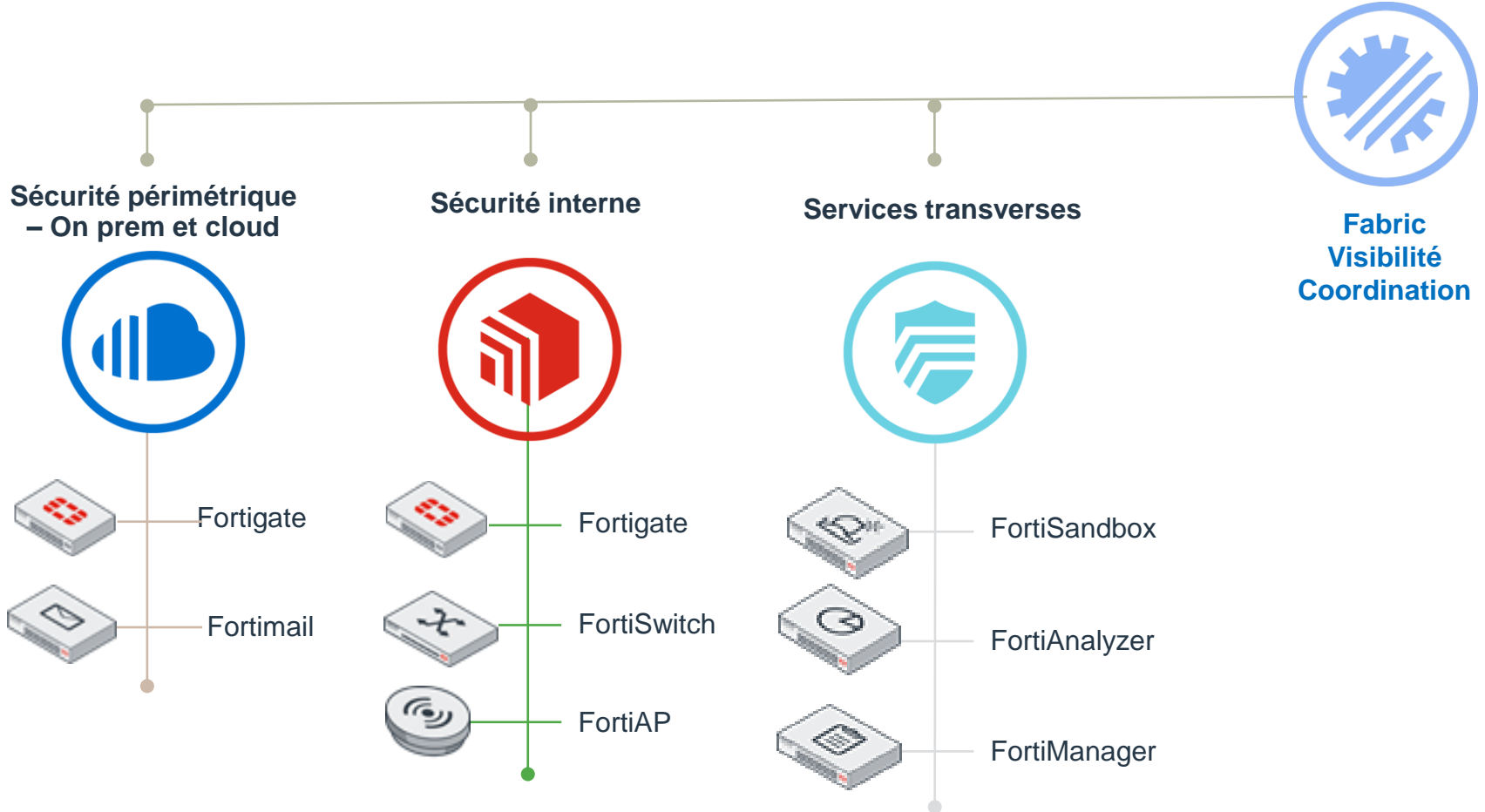
- Visibilité sur l'infrastructure pour gérer le risque efficacement
- Intégration des solutions Fortinet permettant de réduire les contraintes de support de multiples solutions
- Réponse cohérente et automatisée aux attaques sophistiquées



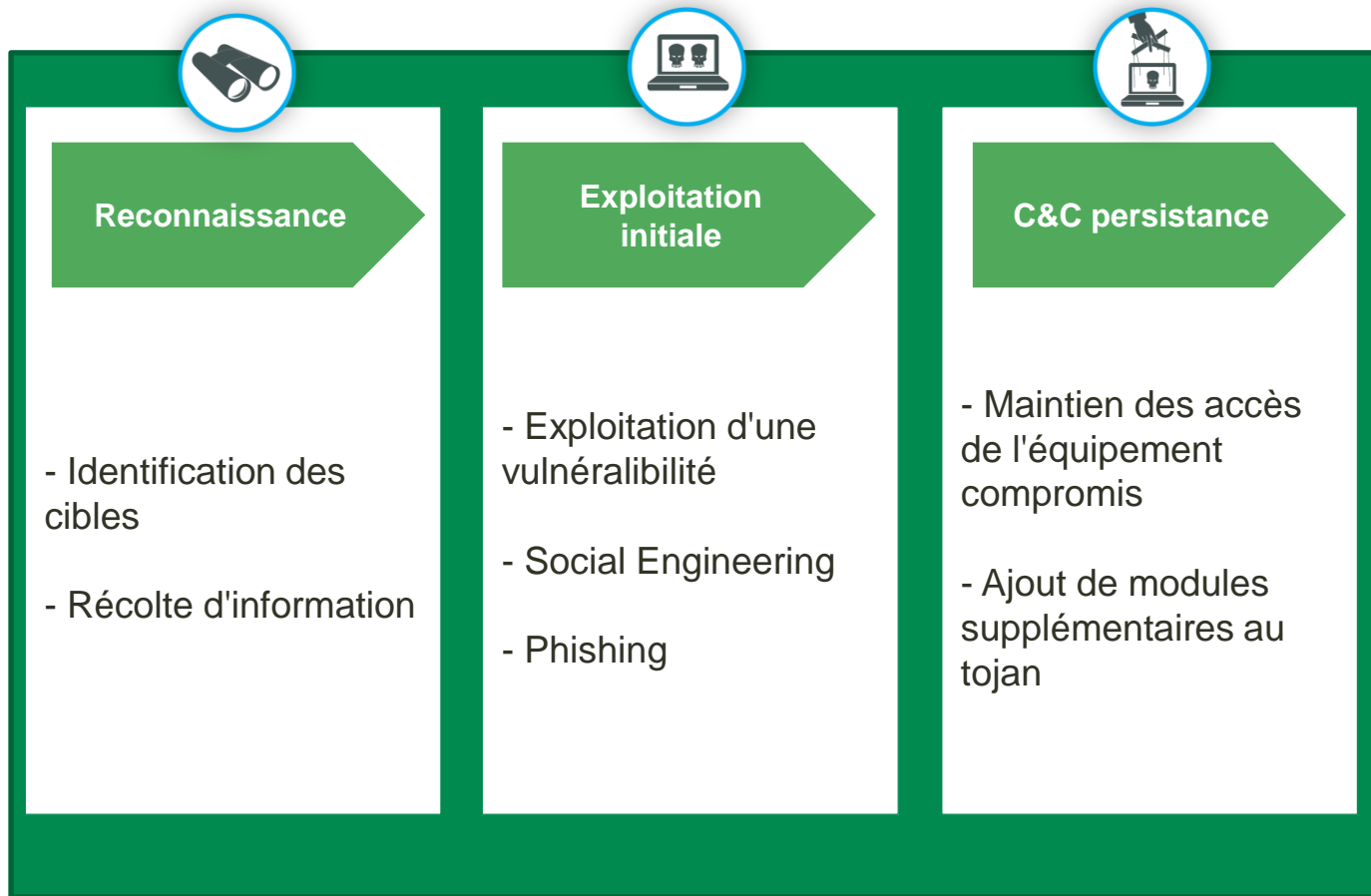
Fortinet Security Fabric – Use Case



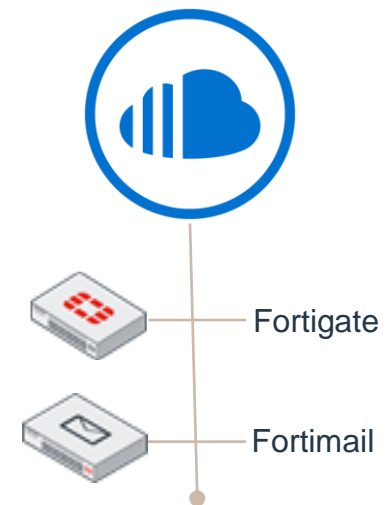
Fortinet Security Fabric – Use Case



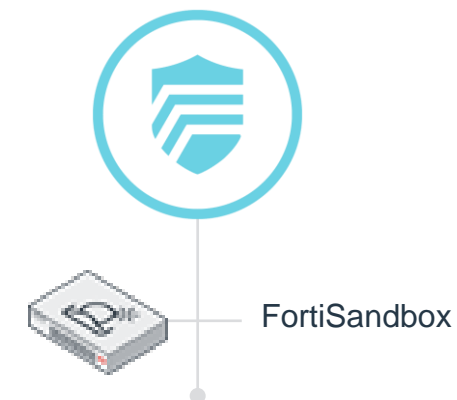
Protection périmétrique



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



99.9%

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



94%

Overall Detection Rate

91%

Protection and Legitimate Handling Rate



99.71%

Spam Catch Rate

94.71%

Malware Catch Rate



99.5%+

Malware Detection Rate

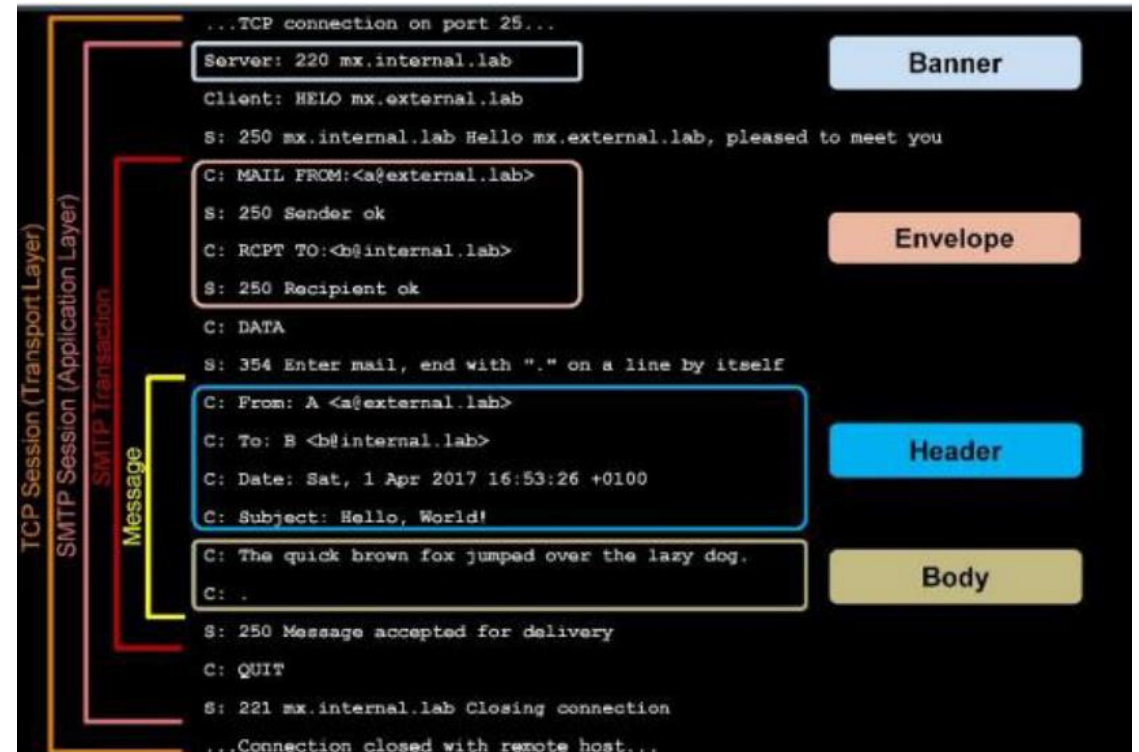
.01%

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

Content Disarm and Reconstruction

Action:

HTML content ⓘ

Text content

MS Office ⓘ

PDF ⓘ

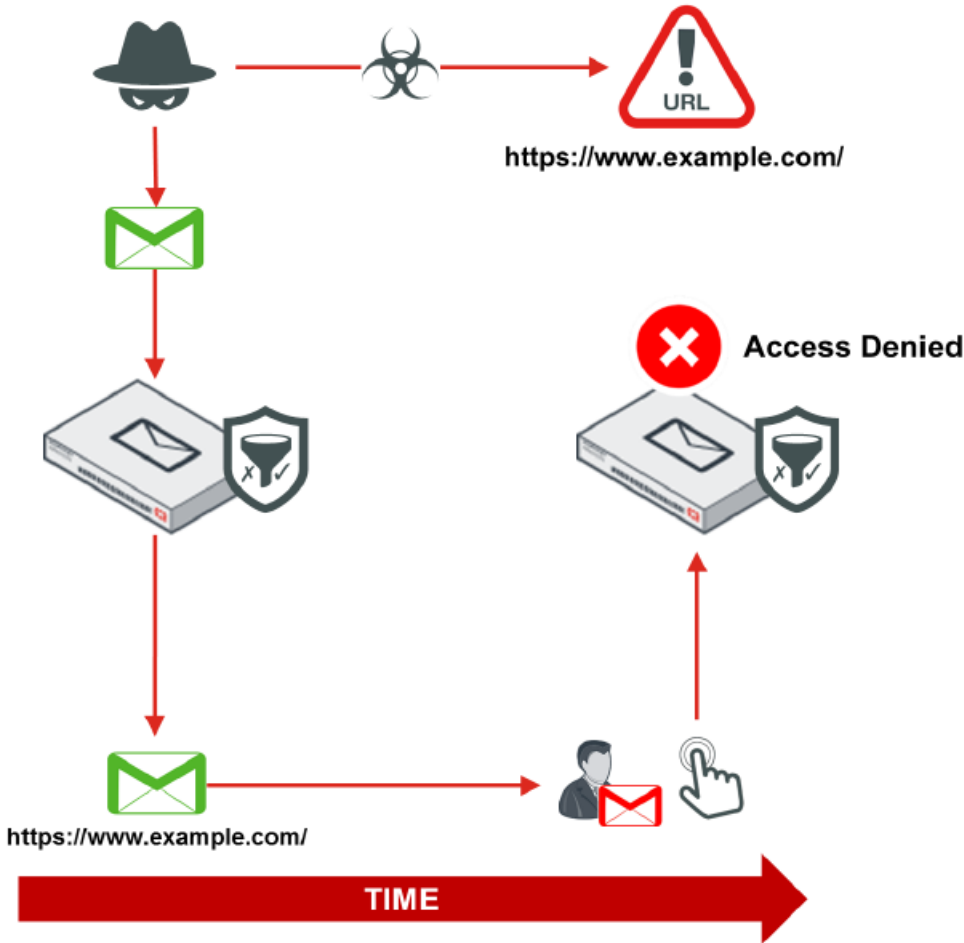
```

...
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



Name <i>i</i>	Regle-Authen-Users-Internet
Incoming Interface	INTERNET (port1) ▼
Outgoing Interface	INTERNAL (port2) ▼
Source	ADD_IP_NTW_CODA_PLO ✕ adm.nav ✕ +
Destination	ADD_FQDN_kms.core.windows.n ✕ +
Schedule	always ▼
Service	HTTPS ✕ +
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN

Firewall / Network Options

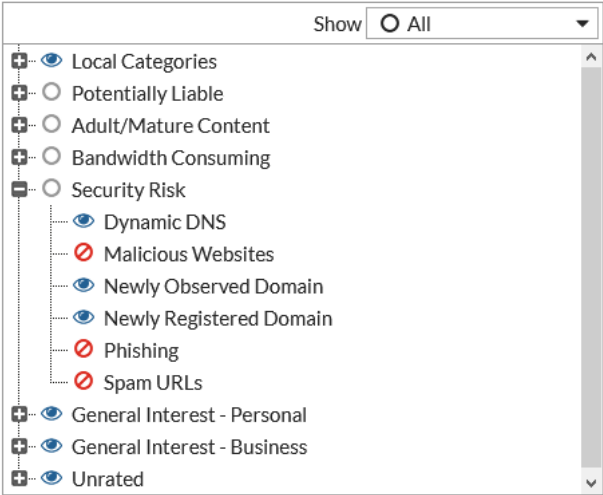
NAT

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port

Protection périmétrique – FortiGate

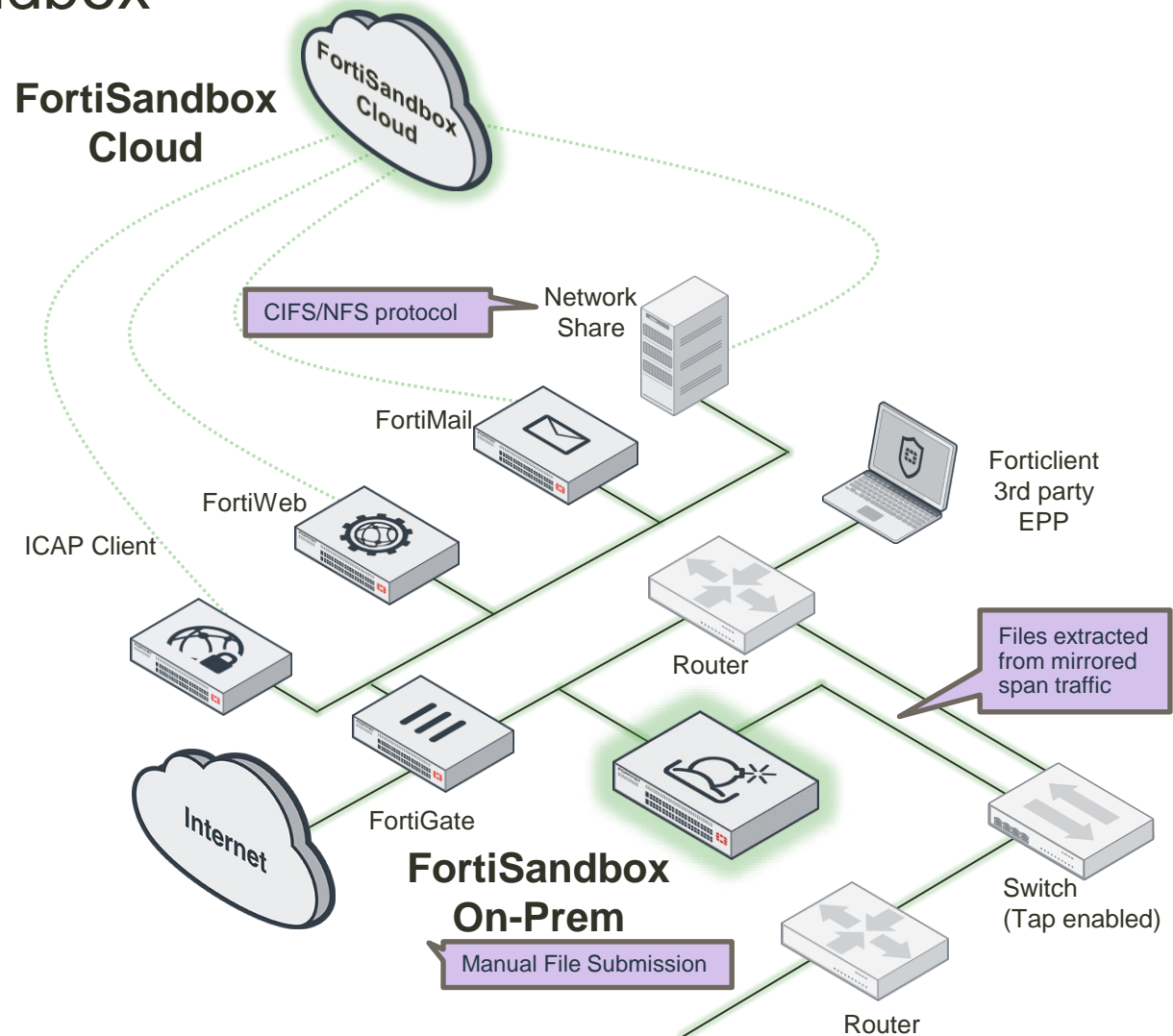
- IPS
- Anti-Virus
- Filtrage Web
- Application control



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.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 environnement 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

FortiSandbox 3000D VM Images admin

VM Images

Edit Clone Number Delete VM Undelete VM VM Screenshot Enabled VM Types: 4 / 4 Keys: 25 / 25 Clone Number: 28 / 28

Name	Version	Status	Enabled	Clone #	Load #	Extensions
Default VMs (2 / 2)						
WIN7X64VM	7	activated	✓	15	15	exe msi wsf upx vbs bat cmd dll ps1 jar pdf swf
WIN7X86VM	6	activated	✓	10	10	pdf pptx ppt pptx xls xlsx doc docx rtf dotx docm dotm xltb xlsb xltm xlsb xlam potx sldx pptm ppsm potm ppam sldm msg dot xlt pps pot pub WEBLINK
Optional VMs (9 / 9)						
AndroidVM	2	activated	✓	2	2	apk
WIN10X64VM	2	installed	✗	0	0	exe msi vbs bat cmd ps1 jar WEBLINK
WIN10X64VMO16	2	installed	✗	0	0	
WIN10X86VM	2	installed	✗	0	0	exe msi bat cmd vbs ps1 jar
WIN7X64SP1	1	installed	✗	0	0	
WIN7X86SP1O16	1	installed	✗	0	0	
WIN81X64VMO16	1	installed	✗	0	0	
WINXPVM	7	activated	✗	0	0	ppsx ppt pptx xls xlsx doc docx rtf dotx docm dotm xltb xlsb xltm xlsb xlam potx sldx pptm ppsm potm ppam sldm msg dot xlt pps pot zip
WINXPVM1	6	activated	✗	0	0	exe
Customized VMs (2)						
win7x64newtool	1	installed	✗	0	0	pdf WEBLINK
win7x64v5	1	activated	✓	1	1	

Protection périmétrique – FortiSandbox

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

The screenshot displays the FortiSandbox analysis interface for document '0A390BC4.vXE'. It features a 'Process Flow' diagram on the left and a detailed view of 'Low Risk Riskware' on the right.

Process Flow:

- AntiVirus Check
- Send to FortiSandbox
- FortiSandbox Scan
- Result

Low Risk Riskware Details:

- Overview | Details | Tree View
- WIN7X86VMO16E
- Behavior Chronology Chart
- Indicators (9)
- MITRE ATTACK (31)

Count	Attack Name	Attack ID	Description	Score	Rating
4	Registry Run Keys / Start Folder	T1060	This file applied low suspicious autostart registry modifications to start itself automatically	30	Low Risk
1	Replication Through Removable Media	T1091	Suspicious AutoRun registry	25	Low Risk
1	Masquerading	T1036	Executable dropped exe file(s) to system directory	25	Low Risk

Additional sections visible in the interface include File Operations (188), Registry Operations (502), Memory Operations (59), and Network Operations (0).

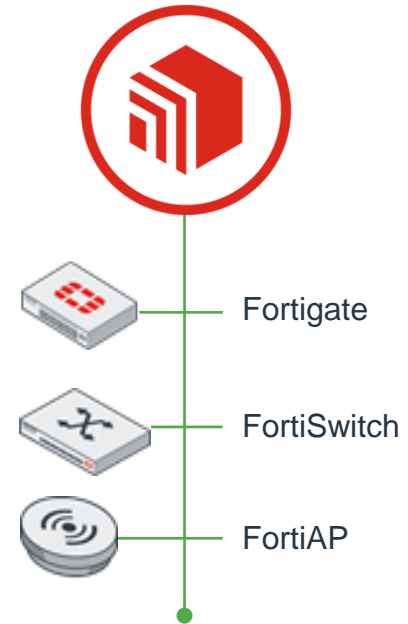
Protection Interne



Mouvement latéral

Utilisation de l'équipement/ comptes piratés pour rebondir dans d'autres zones du système d'information

Sécurité interne

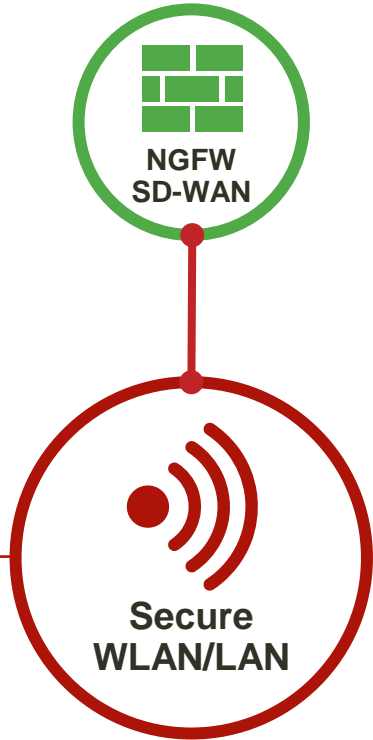


Sécurité interne - Présentation

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

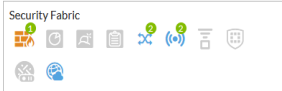
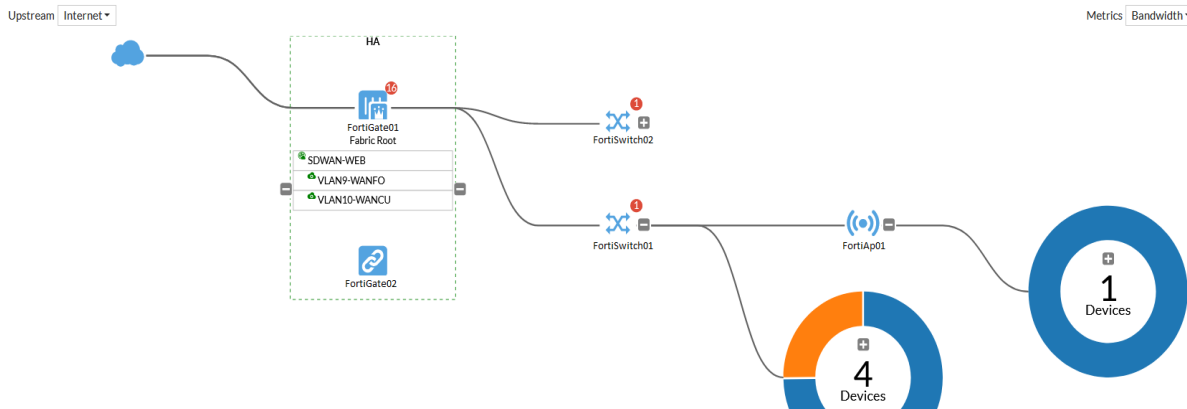


- Etendre la sécurité à la couche access
- Simplifier la gestion



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

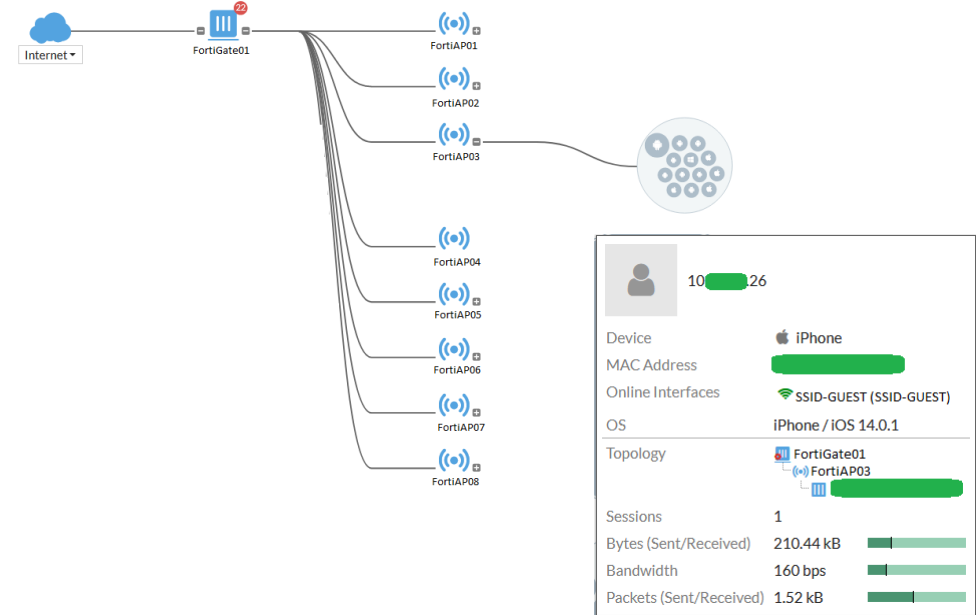


The screenshot shows the FortiGate 100D FortiLink interface. The left sidebar lists various management options, including 'Managed FortiSwitch'. The main area displays a list of managed FortiSwitches, each with its IP address and connection status. A detailed view of a FortiSwitch (S124DF3X16000224) is shown, displaying its configuration, including ports, link status, and power settings.

The screenshot shows a user profile for 'WKS-657'. It displays the device's MAC address, IP address (10.103), and DHCP lease expiration. The user is connected to FortiSwitch01:port5. The profile also shows session statistics: 28 sessions, 3.89 GB of bytes sent/received, 397.72 kbps of bandwidth, and 5.33 MB of packets sent/received. There are buttons for 'Firewall Device Address', 'Firewall IP Address', and 'Quarantine Host'.

FortiAP

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



WiFi & Switch Controller

- Managed FortiAPs
- SSID**
- FortiAP Profiles
- WIDS Profiles
- Security Profile Groups
- Log & Report
- Monitor

Device Detection Active Scanning

WiFi Settings

SSID: Bechtle-demo

Security Mode: WPA2 Personal

Pre-shared Key: Captive Portal

Client Limit: WPA2 Personal

Multiple Pre-shared Keys: WPA2 Personal with Captive Portal

Broadcast SSID: WPA2 Enterprise

Schedule: osen

Block Intra-SSID Traffic:

Broadcast Suppression: ARPs for known clients DHCP Uplink

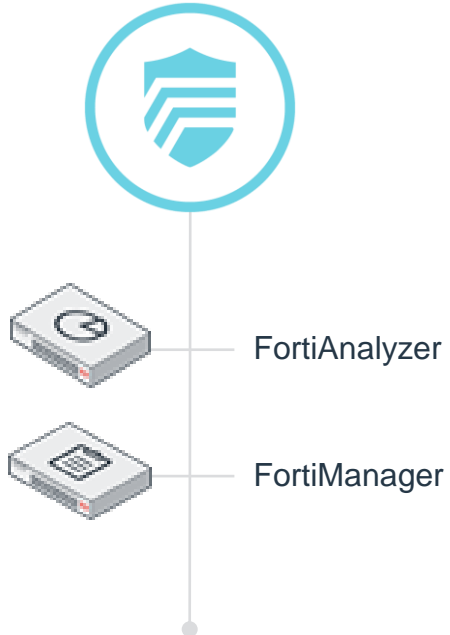
Filter clients by MAC Address

RADIUS server: Local: VLAN Pooling: Quarantine Host:

Visibilité et traçabilité



Services transverses



Visibilité - FortiAnalyzer

FortiAnalyzer – Centralisation log

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



All ADOMs	FortiGates		
Storage Info	FortiCarrier	FortiCarrier	1000 MB
Network	root	FortiGate	233 GB
HA	Other Device Types		
Admin	Chassis	-	-
Administrators	FortiAnalyzer	FortiAnalyzer	1000 MB
Profile	FortiAuthenticator	FortiAuthenticator	1000 MB
Remote Authentication Server	FortiCache	FortiCache	1000 MB
Admin Settings	FortiClient	FortiClient	1000 MB
Certificates	FortiDDoS	FortiDDoS	1000 MB
Local Certificates	FortiMail	FortiMail	1000 MB
CA Certificates	FortiManager	FortiManager	1000 MB
CRL	FortiProxy	FortiProxy	1000 MB
	FortiSandbox	FortiSandbox	1000 MB
	FortiWeb	FortiWeb	1000 MB
	Syslog	Syslog	1000 MB

#	▼ Date/Time	Device ID	Severity	Source	Attack Name	Action
1	16:10:17	FGT9003Z1501	critical	66.240.205.34	Bladabindi.Botnet	dropped
2	15:58:36	FGT9003Z1501	low	199.19.226.67	ZnEu.Vulnerability.Scammer	dropped
3	15:58:31	FGT9003Z1501	low	199.19.226.67	ZnEu.Vulnerability.Scammer	dropped
4	14:55:33	FG1000G1582	critical	120.85.92.135	D-Link.Devices.HNAP.SOAPAction-Header.Command...	dropped
5	14:14:51	FG1000G1582	high	103.82.144.197	Miral.Botnet	dropped
6	13:53:41	FGT9003Z1501	critical	66.240.205.34	MS.Windows.HTTP.sys.Request.Handling.Remote.Cod...	dropped
7	12:00:02	FGT9003Z1501	critical	221.15.239.47	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.C...	dropped
8	10:59:14	FG1000G1582	low	199.19.226.67	ZnEu.Vulnerability.Scammer	dropped
9	10:59:08	FG1000G1582	low	199.19.226.67	ZnEu.Vulnerability.Scammer	dropped
10	10:12:36	FGT9003Z1501	critical	197.3.8.66	Red.Hat.Box.AS.doFilter.Insecure.Deserialization	dropped
11	09:09:51	FGT9003Z1501	low	142.93.123.76	Muleiblackcat.Scammer	dropped
12	09:09:51	FGT9003Z1501	low	142.93.123.76	Muleiblackcat.Scammer	dropped
13	09:09:46	FGT9003Z1501	low	142.93.123.76	Muleiblackcat.Scammer	dropped
14	09:09:46	FGT9003Z1501	low	142.93.123.76	Muleiblackcat.Scammer	dropped
15	09:09:41	FGT9003Z1501	low	142.93.123.76	Muleiblackcat.Scammer	dropped
16	09:09:36	FGT9003Z1501	low	142.93.123.76	Muleiblackcat.Scammer	dropped
17	06:31:26	FGT9003Z1501	critical	93.124.15.205	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.C...	dropped
18	05:16:05	FGT9003Z1501	critical	27.41.6.234	D-Link.Devices.HNAP.SOAPAction-Header.Command...	dropped
19	03:04:00	FGT9003Z1501	high	221.178.127.128	Miral.Botnet	dropped
20	01:55:55	FGT9003Z1501	critical	45.155.205.108	ThinkPHP.Controller.Parameter.Remote.Code.Execution	dropped
21	01:55:55	FGT9003Z1501	high	45.155.205.108	Generic.XXE.Detection	dropped
22	01:48:30	FGT9003Z1501	critical	172.98.64.135	TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Com...	dropped
23	01:27:30	FGT9003Z1501	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped
24	01:27:30	FGT9003Z1501	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped
25	01:26:15	FGT9003Z1501	critical	66.240.205.34	Gh0st.Rat.Botnet	dropped
26	02:02:23:21	FG1000G1582	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped
27	02:02:23:21	FG1000G1582	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped
28	02:02:23:19	FG1000G1582	high	45.155.205.108	Generic.XXE.Detection	dropped
29	02:02:23:19	FG1000G1582	critical	45.155.205.108	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	dropped
30	02:02:23:07	FGT9003Z1501	medium	45.155.205.108	PHP.Discan	dropped
31	02:02:23:07	FGT9003Z1501	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 déjà en place (ServiceNow)

The screenshot shows the FortiAnalyzer Event Manager interface. On the left, there is a navigation menu with options like 'All Events', 'Calendar View', 'Custom View', 'Event Handler List', 'Incidents', 'All Incidents', and 'FortiGate Event Handlers'. The main area displays a table of events with columns for '#', 'Event', 'Event Status', 'Event Type', 'Count', 'Severity', and 'Last Update'. A context menu is open over event #5, showing options: 'Acknowledge', 'Comment', 'View Log', and 'Raise Incident'. The 'Raise Incident' dialog box is open, showing fields for 'Incident Reporter' (pbrown), 'Incident Category' (Malicious Code), 'Severity' (High), 'Status', 'Affected Endpoint', and 'Description'. The 'Severity' dropdown is currently set to 'High'.

#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler
1	FortiCloud activation failed (346)	Event	Event	4009	Medium	7 days ago	A few seconds ago	FortiCloud service activation failed	FCS Event Log Higher Than Warning
2	SSL fatal alert received (143)	Event	Event	5189	Medium	7 days ago	2 minutes ago	SSL Alert received	FCS Event Log Higher Than Warning
3	Admin login failed (172)	Event	Event	1219	Medium	7 days ago	10 minutes ago	...	FCS Event Log Higher Than Warning
4	attack:BlockDevice	Unhandled	IPS	1	Critical	2021-02-03 16:10:17	2021-02-03 16:10:17	General	IPS - Critical Severity
5	IPsec ESP (64)	Event	Event	73	Medium	7 days ago	16 minutes ago	...	FCS Event Log Higher Than Warning
6	Disk quota alert (146)	Event	Event	295	Medium	7 days ago	16 minutes ago	...	Local Device Event
7	SSL Cipher Suites not supported [L...]	Event	Event	151	Medium	7 days ago	37 minutes ago	None of the offered CipherSuites are...	FCS Event Log Higher Than Warning
8	Remove local db (18)	Event	Event	18	Medium	7 days ago	An hour ago	...	Local Device Event
9	Trim local db (18)	Event	Event	18	Medium	7 days ago	An hour ago	...	Local Device Event
10	D-Link.Devices.HNAPS.OAIPAction...	Mitigated	IPS	16	Critical	6 days ago	An hour ago	OS Command Injection (CVE-2015-2...	IPS - Critical Severity
11	User login failed (63)	Event	Event	85	Medium	7 days ago	2 hours ago	...	Local Device Event
12	Configuration changed (2)	Event	Event	4	Medium	7 days ago	2 hours ago	Configuration is changed in the ad...	FCS Event Log Higher Than Warning
13	Missed Session (14)	Event	Event	16	High	7 days ago	2 hours ago	General	IPS - High Severity
14	Disk quota is reached (60)	Event	Event	40	Medium	7 days ago	2 hours ago	...	FCS Event Log Higher Than Warning
15	SSL decryption failed (18)	Event	Event	30	Medium	7 days ago	2 hours ago	SSL decryption failure	FCS Event Log Higher Than Warning
16	SSL fatal alert sent (18)	Event	Event	30	Medium	7 days ago	2 hours ago	SSL Alert sent	FCS Event Log Higher Than Warning
17	MS.Windows.HTTP.sys.Request.L...	Mitigated	IPS	16	Critical	7 days ago	3 hours ago	Buffer Errors (CVE-2015-1635)	IPS - Critical Severity
18	_cmdesc:Phishing	Mitigated	Web Filter	13	Medium	2021-02-03 12:40:33	2021-02-03 12:51:48	Security Risk	UTM Web Filter Event
19	NETGEAR.DGN1000.CCCLUnauth...	Mitigated	IPS	20	Critical	6 days ago	4 hours ago	Code Injection	IPS - Critical Severity
20	Delete log file (6)	Event	Event	6	Medium	6 days ago	6 hours ago	...	Local Device Event
21	attack:Root.Hat_Bases.AS.dof.Rer...	Mitigated	IPS	1	Critical	2021-02-03 10:12:36	2021-02-03 10:12:36	OS Command Injection (CVE-2017-1...	IPS - Critical Severity
22	Disk log file deleted (99)	Event	Event	409	Medium	7 days ago	10 hours ago	...	FCS Event Log Higher Than Warning
23	Progress IPsec phase 1 (42)	Event	Event	49	Medium	7 days ago	12 hours ago	progress IPsec phase 1	FCS Event Log Higher Than Warning
24	Heartbeat device interface down L...	Event	Event	12	Medium	7 days ago	14 hours ago	Heartbeat device/interface down	FCS Event Log Higher Than Warning
25	ThinkPH@Controller.Parameters...	Mitigated	IPS	20	Critical	7 days ago	14 hours ago	Code Injection (CVE-2019-0082,CVE...	IPS - Critical Severity
26	Generic_XSS.Detection (4)	Mitigated	IPS	4	High	4 days ago	14 hours ago	Other (CVE-2012-3363,CVE-2013-4...	IPS - High Severity
27	attack:TrueOnline.ZyKEL.P660RNLV...	Mitigated	IPS	1	Critical	2021-02-03 01:48:30	2021-02-03 01:48:30	Code Injection (CVE-2017-18368)	IPS - Critical Severity
28	PHPMailer.send_mail.PHP.Banned.C...	Mitigated	IPS	82	Critical	7 days ago	15 hours ago	Code Injection (CVE-2017-9841)	IPS - Critical Severity

Visibilité - FortiAnalyzer

FortiAnalyzer – SOC & NOC

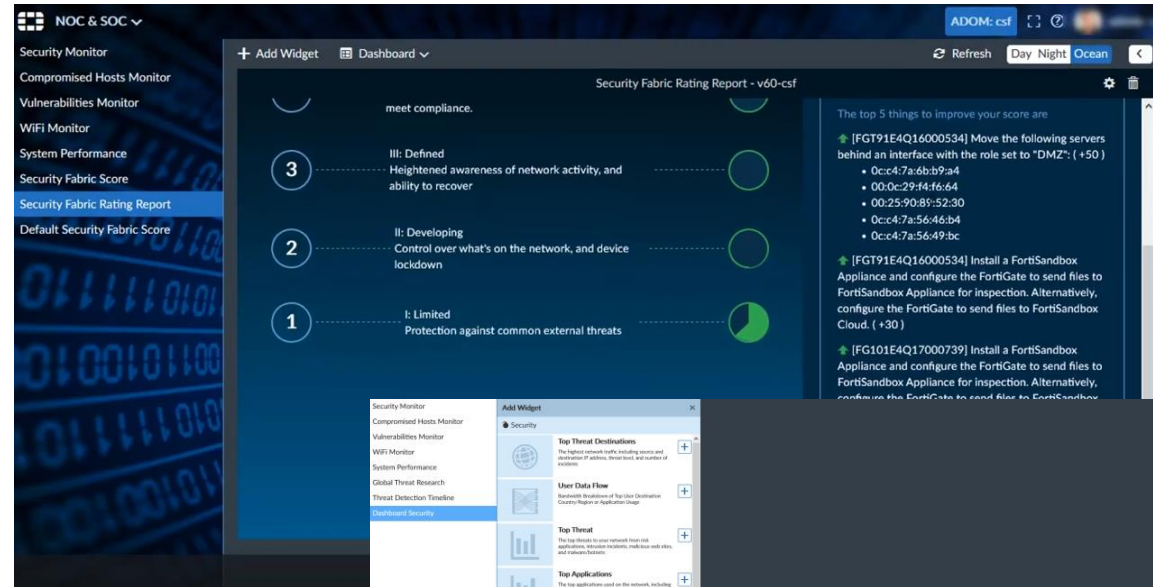
■ Fonctionnalité Noc / Soc permet d'avoir un état des lieux de votre infrastructure

- 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

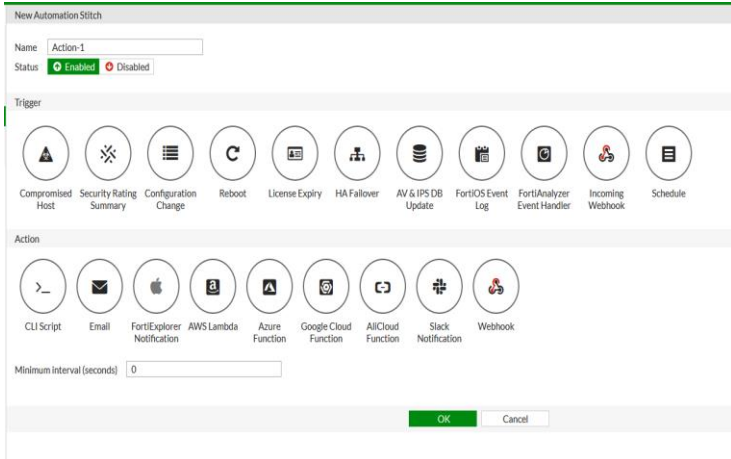
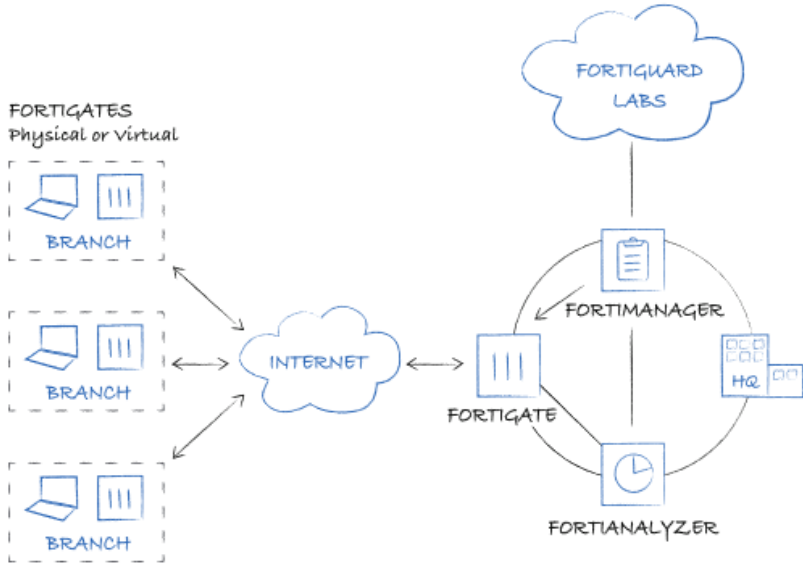
Intrusions Detected

#	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.SOAP.Action-Header.Command.Execution	Critical	CVE-2015-2051,CVE-2019-10891	15
9	Telarik.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

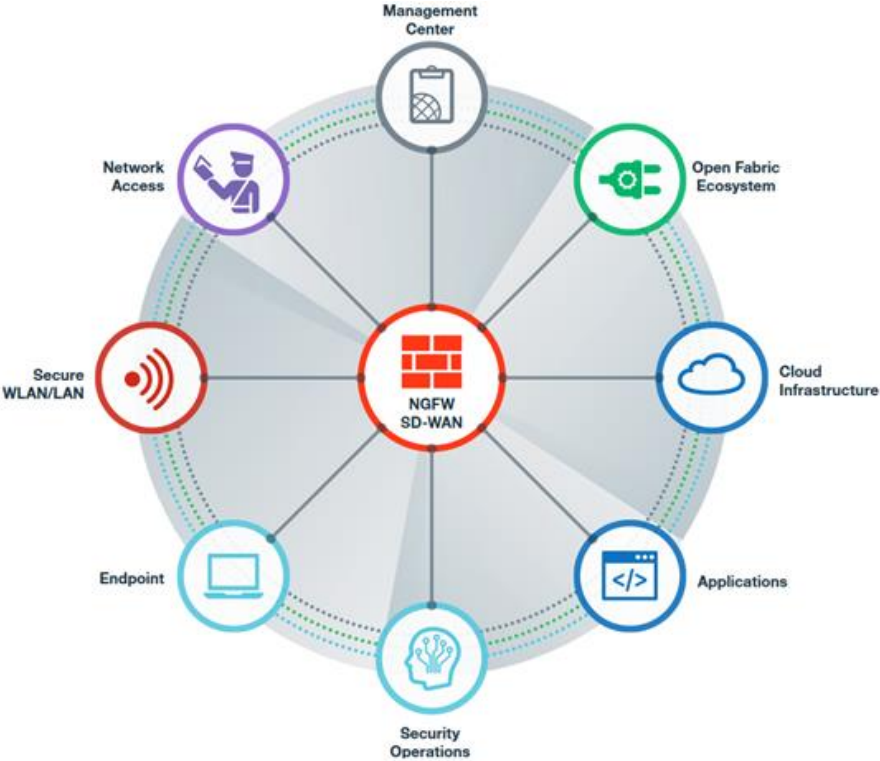
- Multi-Plateforme
- Management centralisé :
 - Règles de filtrage et bases d'objets communes
 - Mises à jour des équipements
 - Sauvegardes des équipements
- Workflow / Orchestration
 - Automatisation



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)

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

The image displays three components of the Fortinet Cyber Threat Assessment Report:

- Cover Page:** Features the Fortinet logo and three hazard icons (biohazard, cloud, and a person with a lightning bolt). The title is "Cyber Threat Assessment Report".
- Recommended Actions Page:** Contains sections for:
 - Application Vulnerability Attacks Detected (49):** Application vulnerabilities (also known as CVEs) act as entry points used to gain security information and allow attackers a foothold into your organization.
 - Malware Detected (6):** Malware can take many forms: viruses, trojans, spyware, worms, etc. Any intrusion of malware detected means security on the network could also include a threat actor originating from inside the organization, often unwittingly.
 - Botnet Infections (1):** Bots can be used for launching denial-of-service (DDoS) attacks, distributing spam, spreading and stealing, propagating malware, and harvesting confidential information which can lead to serious financial and legal consequences.
 - Malicious Websites Detected (125):** Malicious websites are often linked to host malware where it is designed to covertly collect information, damage the host computer, or otherwise manipulate the target machine without the user's consent.
 - Phishing Websites Detected (1):** Similar to malicious websites, phishing websites imitate the webpage of legitimate websites in an effort to collect personal or private information, passwords, etc. Information from phishing websites are often linked to other malicious scripts sent to your organization.
 - Proxy Applications Detected (5):** These applications are used to bypass or circumvent security measures. For instance, users may circumvent the firewall by bypassing or encrypting external communications. In many cases, this can be considered a willful act and a violation of corporate use policies.
 - Remote Access Applications Detected (4):** Remote access applications are often used to access external hosts remotely (via logging, NAT or providing a secondary access path) bypassing or circumventing security measures. Remote access can be used to facilitate data exfiltration and increase espionage activity. Many times, the use of remote access is unmonitored and/or manual corporate use changes should be put into practice.
 - POP and Hijacking Applications (2):** These applications can be used to bypass existing content controls and/or to circumvent data transfer and data policy restrictions. Policies on appropriate use of these applications need to be implemented.
- High Risk Applications Page:** Titled "Security and Threat Prevention High Risk Applications". It includes a table of high risk applications:

#	App. Application Name	Category	Technology	User	Bandwidth	Devices
1	Outlook	Outlook	Client Server	1	22,719.00	33
2	Microsoft	Proxy	Client Server	30	275,70.00	31
3	Outlook Basic/Exchange	Proxy	Client Server	1	11,22.00	14
4	Outlook	Proxy	Client Server	3	25,81.00	10
5	Outlook	Proxy	Client Server	3	7,93.00	9
6	Outlook	Proxy	Client Server	1	88.0	1
7	Outlook	Proxy	Client Server	1	44.0	1
8	Outlook	Proxy	Client Server	1	13,72.00	108
9	Outlook	Proxy	Client Server	1	1,41.00	30
10	Outlook	Proxy	Client Server	1	5.00	14
- Application Vulnerability Exploits Page:** Titled "Application Vulnerability Exploits". It includes a table of top application vulnerabilities:

#	Severity	Event Name	Type	Metric	Source	Count
1	Critical	Exploit/Buffer Overflow/Buffer Overflow	Buffer Overflow	4	3	20
2	Critical	Exploit/Buffer Overflow/Buffer Overflow	Buffer Overflow	1	1	3
3	Critical	Exploit/Buffer Overflow/Buffer Overflow	Buffer Overflow	1	1	30
4	Critical	Exploit/Buffer Overflow/Buffer Overflow	Buffer Overflow	1	1	2
5	Critical	Exploit/Buffer Overflow/Buffer Overflow	Buffer Overflow	1	1	2
6	Critical	Exploit/Buffer Overflow/Buffer Overflow	Buffer Overflow	1	1	2
7	Critical	Exploit/Buffer Overflow/Buffer Overflow	Buffer Overflow	1	1	2
8	Critical	Exploit/Buffer Overflow/Buffer Overflow	Buffer Overflow	1	1	2
9	Critical	Exploit/Buffer Overflow/Buffer Overflow	Buffer Overflow	1	1	2
10	Critical	Exploit/Buffer Overflow/Buffer Overflow	Buffer Overflow	1	1	2

Accelerate 2021 EMEA Digital Edition - March 10, 2021

FORTINET

ACCELERATE 2021

ONE VISION

Save the Date

Accelerate 2021 Digital Edition

March 9th AMERICAS
March 10th EMEA ←
March 11th APAC/JAPAN

JOIN US FOR ACCELERATE 2021

The poster features a dark blue header with the Fortinet logo. The main content is on a light grey background with a large, stylized 'ONE VISION' graphic. Below this, the event dates are listed, with a red arrow pointing to 'March 10th EMEA'. On the right, there is a photograph of a modern city street with a person walking. The bottom of the poster has a dark blue footer with the text 'JOIN US FOR ACCELERATE 2021' in orange.

Any questions?

chithavong.chokbengboun@bechtle.com

sylvain.pionchon@bechtle.com

Learn more at
bechtle.com

