CYBER THREAT ASSESSMENT PROGRAM (CTAP)

DNS & Fortinet

Přední výrobce zabezpečení IT infrastruktury společnost **Fortinet** pro partnery připravila podpůrný program „**Cyber Thread Assessment Program**“ (CTAP). Výstupem programu CTAP je přehledný report, který přináší obchodním partnerům zajímavý nástroj, jak zákazníkům bezplatně zajistit bezpečnostní audit a tím jim odhalit reálný stav a faktickou úroveň zabezpečení jejich datové infrastruktury. CTAP report koncovým zákazníkům ukáže kolik a jakých bezpečnostních hrozeb, škodlivého kódu, kritických aplikací a jaká data se na jejich síti aktuálně vyskytují. Jaká jsou naše doporučení nápravy a co všechno umíme na technologiích Fortinet zachytit a eliminovat v případě implementace u zákazníka.

CTAP auditní program je od nás distributora **DNS a.s.** plně technicky a materiálně podporován. Jsme připraveni, našim partnerům pomoci k snadnému přístupu a získání velice užitečného reportu bez zbytečných nákladů a s minimální pracností. Máme pro vás na skladě k zapůjčení několik kusů menších boxů, které jsou kompatibilní pro nasazením u zákazníka v režimu **Cloud CTAP**. Jsme připraveni vám tyto zařízení zapůjčit a pomoci vám nejen technicky s celým programem. Věříme, že sami brzy zjistíte, jak je tento program skvěle a jednoduše připraven a doba konfigurace i nasazení nezabere více jak hodinu. Maximální efektivita je dosažena především díky vysoké míře automatizace, která vygeneruje samotnou konfiguraci, dále vygeneruje dokument k fyzickému zapojení, spustí v Cloudu všechny potřebné nástroje, aby i pro naprosto neznalého a nepolíbeného člověka, to nebyl žádný problém.

Dalším motivačním benefitem programu CTAP pro partnery, je možnost, kvartálně získat odměnu **až 250 USD** za prodej zařízení na základě realizovaného CTAP programu. Prodané zařízení musí být v minimální hodnotě cca 120 tisíc CZK bez DPH.

CTAP report, je výstupem a analýzou provozních síťových logů generovaných především zařízením **FortiGate**, které ologuje provoz interními nástroji a mechanismi. Tyto logy odešle analytické platformě **FortiAnalyzer** (https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf/), která zajistí vyhodnocení logů a zpracuje finální report za daný časový úsek. Doporučením pro délku sběru informací, tak aby to byl dostatečný a representativní vzorek, je nechat CTAP běžet 1-2 týdny. Tento časový interval je ovšem pouze doporučením, které zaleží v první řadě na místních možnostech a potřebách zákazníka, např. z důvodu pravidelných zálohování, aktualizací systémů atd.. FortiAnalyzer, poskytuje nejen logovací, ale především, analytickou, automatizační a integrační platformu pro různé produkty Fortinet technologií. Pro partnery je možná Free licence, pro jejich vzdělávací a jiná využití, pro více informací nás případně kontaktuje.

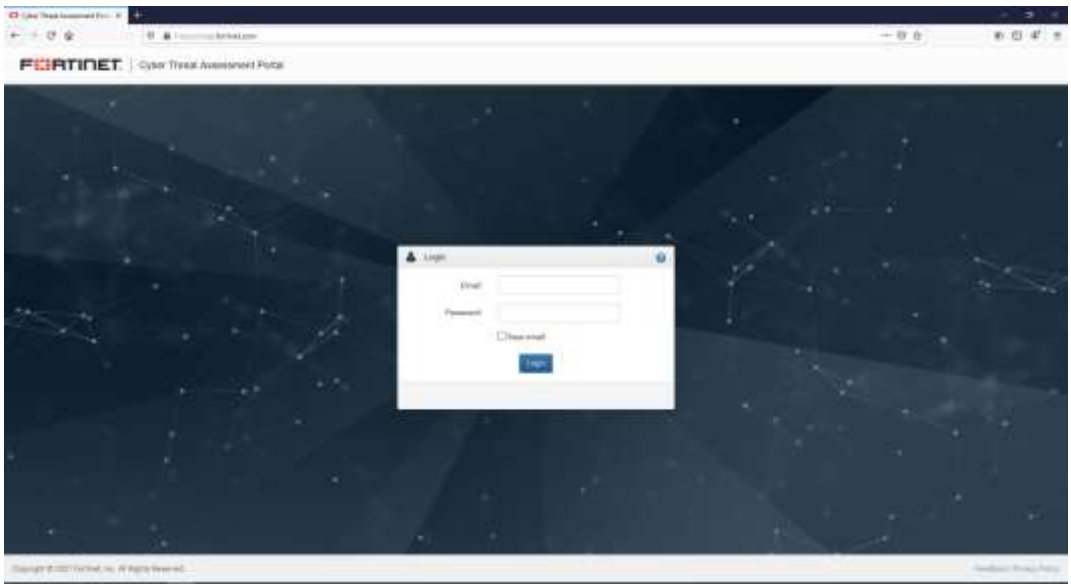
Portfolio produktů obsahuje širokou paletu variant, jak FortiGates, ale i dalších produktů FortiEmails a to i velkou variací FortiAnalyzers (HW, VM, Cloud), přináší nespočet možností samotného nasazení. Máme pro vás pokrytí i pro zákazníky, kteří chtějí mít vše u sebe na síti a neposílat nic do Cloudu. I různé rozdílné implementace a nasazení u zákazníka. S tím jsou ovšem spojeny související další požadavky na součinnost zákazníka atd., proto se v tomto dokumentu zaměříme především na **Cloud CTAP**, který je nejméně pracný, s minimem nákladů a pro 95% zákazníků v České Republice.

U zákazníka Cloud CTAP vyžaduje fyzicky: konektivitu s interním provozem – “ologování“ pro analýzu

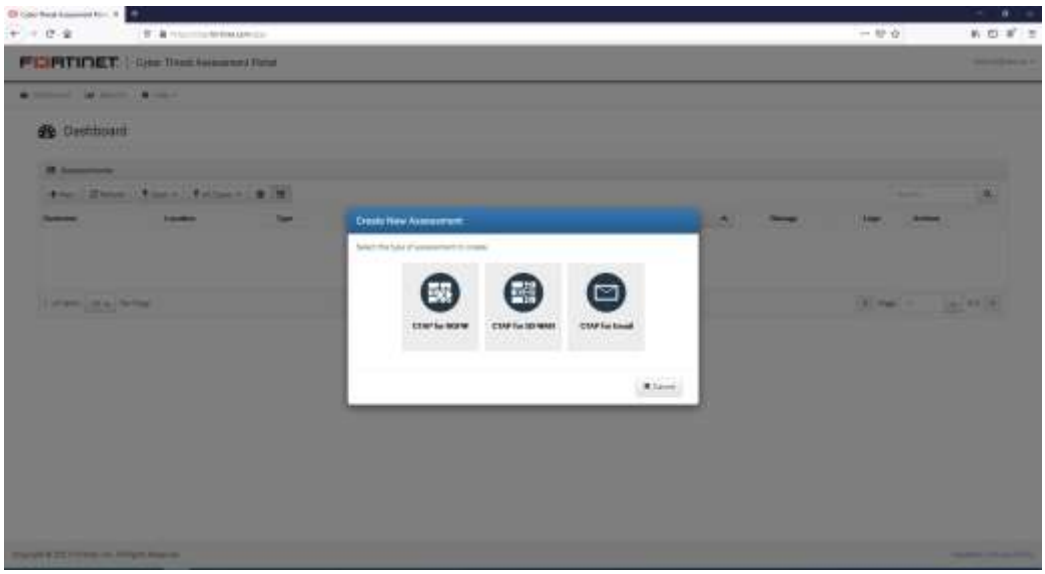
konektivitu do internetu – pro zaslání logů k analýze

Cloud CTAP programy

Cloud CTAP portál je pro partnery dostupný na **https://ctap.fortinet.com/** a jedná se o nejjednodušší způsob, jak zajistit CTAP report pro koncového zákazníka. Účet na **https://ctap.fortinet.com/** je to provázané s účtem na https://partnerportal.fortinet.com/ .



Reálně tento způsob vyžaduje pouze zapojení jednoho FortiGate do zákaznické sítě. Na portále má každý CTAP program vyčleněno úložiště pro logy v objemu 20GB a je možné si navolit libovolně délku samotného programu. CTAP funguje na principu analýzy logů, které jsou generovány síťovým zařízením od společnosti Fortinet a odeslány k analýze na FortiAnalyzer. Cloud portál nabízí tři základní oblasti

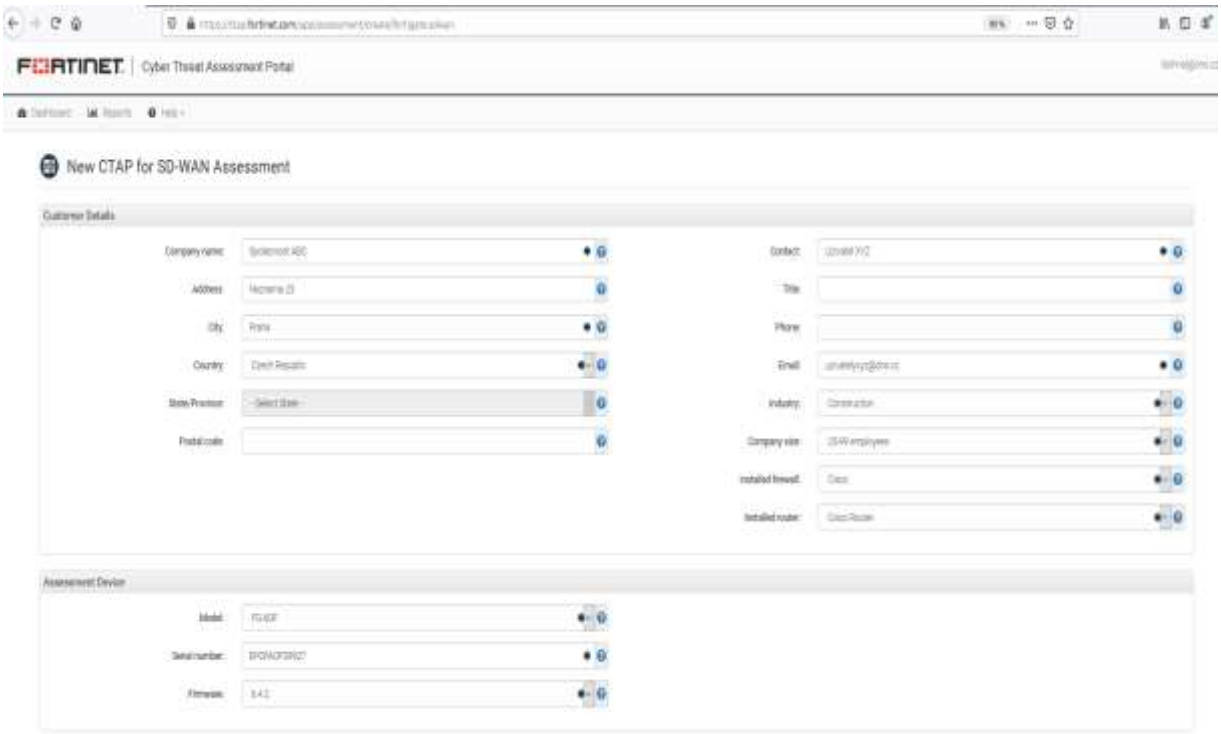


CTAP na NGFW – náš klíčový program na bázi síťového firewall **FortiGate,** je zaměřen především na prověření služeb na bázi (IPS Service, App Control Service, Advanced Malware Protection, Antivirus, Antispam, Mobile Malware, Botnet, CDR, Virus Outbreak Protection, Web&Video Filtering). Po vyplnění krátkého formuláře, který je společný pro programy NGFW a SD-WAN, poté dojde k vygenerování potřebných konfigurací a všech potřebných náležitostí. Podrobněji se zaměříme na několik podstatných položek povinných polí (*).

CTAP na SD-WAN – program pokrývá stejnou paletu služeb jako CTAP NGFW, implementace u je rozšířeno o služby SD-WAN. Kdy je ám dává doporučené na zlepšení možností pro jednotlivé aplikace v návaznosti na využití linek na principech QoS.

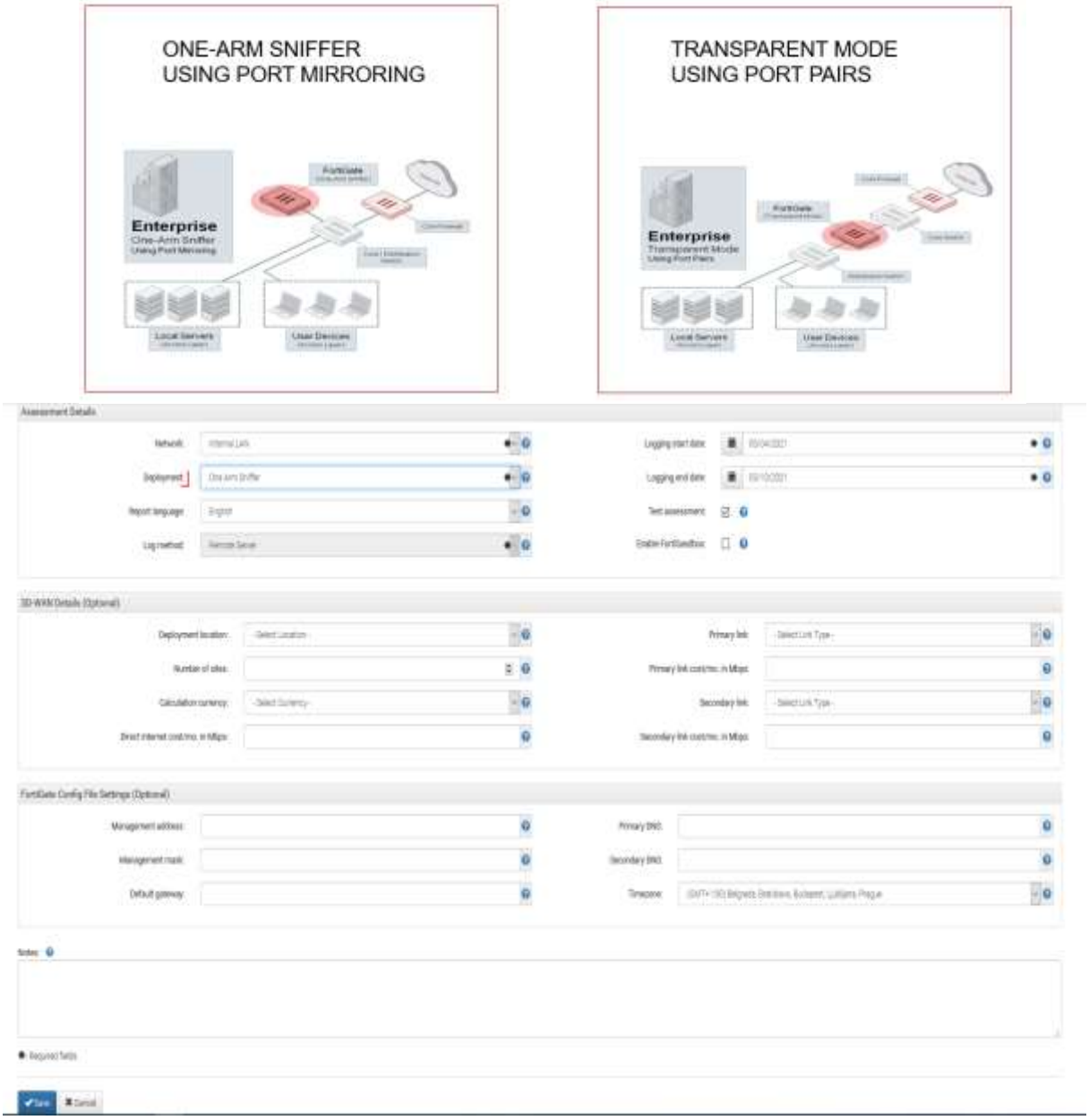
CTAP na Email – program pokrývá stejné služby, jako NGFW s důrazem na služby SD-WAN, kdy nám dává doporučené na zlepšení možností pro jednotlivé aplikace v návaznosti na využití linek na principech QoS.

Příklad formuláře CTAP SD-WAN v módu One Arm Sniffer



Velice důležité je pole **Deployment** a které zásadním způsobem určuje, jaké bude fyzické i logické zapojení a celkovou realizaci!
One Arm Sniffer – tato volba znamená snadný a plně pasivní způsob analýzy, kdy je FortiGate napojen na infrastrukturu zákazníka s pomocí nazrcadlení komunikace. Tento způsob je velice bezpečný bez možného ovlivnění stávající komunikace.

Transparent Mode – v tomto zapojení, je Fortigate předřazen a zapojen do stávající infrastrůktury a živá data protékají skrze



V případě, že máme některý podporovaný FortiGate s lokálním diskem (FG100D, FG61F apod.), můžeme si zvolit metodu nejprve logovat na lokální disk a následně zaslat na analýzu do FortiCloudu. V našem vzorovém případě máme model FG60F, který nemá lokální disk, volba je automaticky “Remote Server”. Jakmile dojde k vyplnění všech důležitých polí, dojde k vygenerování virtuálního prostředí a konfigurací. Následně je možné připojit nakofigurovaný FortiGate do sítě a začít se sběrem logů.

Oblasti analýzy

BEZPEČNOST & PREVENCE HROZEB

PRODUKTIVITA UŽIVATELŮ

ZATÍŽENÍ SÍTĚ

Bezpečnost a prevence hrozeb

- Efektivita aktuální síťové bezpečnosti
- Zranitelnost aplikací
- Malware/Botnet detekce
- „At Risk“ zařízení v síti

Produktivita uživatelů

- Přehled užívání aplikací a webu v síti
- Podíl peer to peer, sociálních síti, chatovacích utilit v rámci provozu
- Využití client – server a webových aplikací v rámci korporátní politiky

Zatížení sítě

- Optimalizace sítě
- Throughput, session a bandwith využití během špičky provozu
- Návrhy řešení bezpečnosti na základě aktuálního provozu

Podporované HW platformy a verze FortiOS

Model	Versions
FG-60E	6.0.2, 6.0.7, 6.2.3, 6.4.1
FG-60F	6.4.2
FG-61F	6.4.2
FG-100D	5.6.5
FG-300D	5.6.5
FG-300E	6.0.2, 6.2.3, 6.4.1
FG-400E	6.4.1
FG-1100E	6.4.1
FG-1101E	6.4.1
FG-1500D	5.6.5
FG-VM (ESXi)	6.4.1

FortiGate 60F

FortiGate 300E

BOX	60F
Propustnost firewallu	10 Gbps
Latence	4 µs
Připojení za vteřinu	35 000
Souběžných připojení	700 000

BOX	300E
Propustnost firewallu	32 Gbps
Latence	37 µs
Připojení za vteřinu	300 000
Souběžných připojení	4 000 000

FortiGate 1500D

BOX	1500D
Propustnost firewallu (Mbps)	80 Gbs
Latence	3 µs
Připojení za vteřinu	300 000
Souběžných připojení	12 000 000

Soupis kroků k nasazení u zákazníka

Pro využití této služby se přihlaste prostřednictvím partnerského portálu společnosti Fortinet – https://ctap.fortinet.com/ a před zahájením testování zadejte požadavek na vytvoření reportu.

1. Na webovém portálu se pod položkou *Help* (v pravém horním rohu) stáhne kompletní konfigurace pro daný FortiGate v konkrétní verzi FortiOS (5.2 nebo 5.4).
2. Do FortiGate v režimu „tovární nastavení“ se provede *restore* této stažené konfigurace.
3. Nasazení probíhá ve dvou variantách:
    a. Mezi stávající firewall a páteřní switch LAN se do portů 1 a 2 zapojí FortiGate, který začne prohlížet datový tok procházející přes porty a z celého provozu zaznamenává Fortigate log.
    b. Na portu 4 je nakonfigurovaný *ONE-ARM Sniffer* port, který se zapojí do přednastaveného *mirror* portu páteřního switche. Opět je prováděno logování celého datového provozu (v tomto nastavení se musí počítat s větším zatížení páteřního switche).
4. Po 7. denním monitorování provozu uloží administrátor celý log z FortiGate a provede *upload* na webový portál https://ctap.fortinet.com/. Po několika dnech je zde k dispozici kompletní report ke stažení.

Vzor CTAP SD-WAN reportu:

https://www.fortinet.com/content/dam/fortinet/assets/intelligence-reports/sample-report-sdwan-threat-assessment.pdf

V tomto dokumentu se nevěnujeme CTAP na Email, ani jiným možnostem implementací, proto se na nás v případě, že uvedený dokument nepokrývá vaše potřeby, neváhejte obrátit na technickou konzultaci a pro další informace.

Kontaktní osoby

Produktový manažer	Daniel Kosňanský	Vojtěch Krak	Ondřej Novák
	dkosnansky@dns.cz 724 222 171	vkrak@dns.cz 724 345 532	onovak@dns.cz 776 652 318
Technický konzultant	Filip Hájek	Lukáš Dohnal	Jan Nguyen
	fhajek@dns.cz 724 384 428	ldohnal@dns.cz 730 189 089	jnguyen@dns.cz 724 222 169