
NETIA
netianext
Dziękuję.
Paweł Szymkowicz
Kierownik Działu Utrzymania Usług ICT
FORTINET
EXCLUSIVE NETWORKS

Raporty

NETIA
netianext

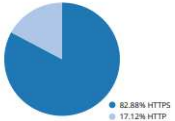
Top 20 Categories By Bandwidth

#	Category
1	Information Technology
2	Streaming Media and Download
3	Business
4	Social Networking
5	Content Servers
6	Search Engines and Portals
7	File Sharing and Storage
8	Internet Radio and TV
9	Advertising
10	Unrated
11	Web-based Email
12	Shopping
13	Reference
14	Web-based Applications
15	Finance and Banking
16	Freeware and Software Downloads
17	Travel
18	Pornography
19	Games
20	News and Media

Botnet Detected

#	Botnet Name
1	RedLine.Stealer.Botnet
2	Mirai.Botnet
3	Bladabindi.Botnet
4	Gh0st.Rat.Botnet
5	SystemBC.Botnet
6	Zeroaccess.Botnet

HTTP SSL Traffic Ratio



Intrusions Detected

#	Attack Name	Severity	CVE-ID
1	Zyxel.Firmware.error.message.Command.Injection	Critical	
2	TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Command.Injection	Critical	CVE-2017-18368
3	Apache.Log4j.Error.Log.Remote.Code.Execution	Critical	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046
4	Netcore.Netis.Devices.Hard coded.Password.Security.Bypass	Critical	
5	Realtek.SDK.UDPServer.Command.Execution	Critical	CVE-2021-35394
6	Remote.CMD.Shell	Critical	
7	Bladabindi.Botnet	Critical	
8	Gh0st.Rat.Botnet	Critical	
9	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Critical	CVE-2019-9082,CVE-2018-20062
10	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Critical	CVE-2017-9841

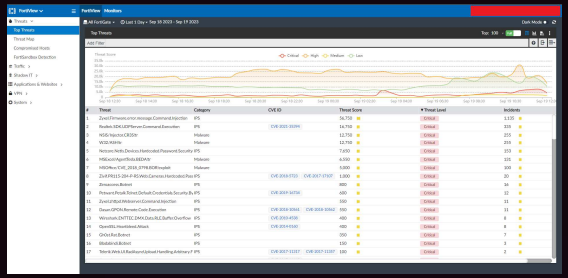
FortiAnalyzer > FortiSOC

NETIA
netianext

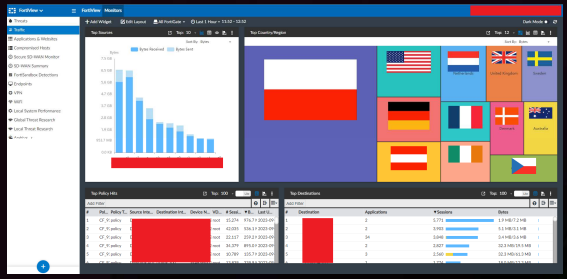
- SOC automation
- Outbreak Alerts
- Incident and Event Management
- Reports

Narzędzia

NETIA
netianext



FortiAnalyzer API FortiManager



Jakimi usługami zarządzamy?

NETIA
netianext

- Netia Cloud Firewall
- Netia Managed UTM
- Netia Incident Monitoring
- Netia (Secure) SD-WAN+

UTM a bezpieczeństwo

NETIA
netianext

From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: Szymkowicz Paweł <Pawel.Szymkowicz@netia.pl>
Subject: Rekonfiguracja LAN

Dzień dobry,

Podstawowym zadaniem do wykonania jest segmentacja sieci. Aktualnie Państwa sieci LAN ma płaską strukturę, gdzie wszystkie urządzenia serwery, kamery, komputery są w jednej wspólnej sieci 192.168.11.0/24.
Zalecamy aby podzielić infrastrukturę na kilka segmentów stosując dla nich osobne sieci i VLAN. Do tego celu dodatkowo niezbędny będzie zarządzany przełącznik z obsługą VLAN.

Przykład segmentacji LAN:
LAN Serwery: 10.1.1.0/24
LAN Backup/NAS: 10.2.2.0/24
LAN Kamery: 192.168.8.0/24
LAN Pracownicy: 192.168.10.0/24
LAN Wifi: 192.168.12.0/24
VPN: 10.212.134.0/24

Powyższe niesie za sobą konieczność ustalenia polityk bezpieczeństwa pomiędzy sieciami, tzn. kto i do czego ma mieć dostęp i dla jakich portów/protokołów.

UTM a bezpieczeństwo

NETIA
netianext

From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: Szymkowicz Paweł <Pawel.Szymkowicz@netia.pl>
Subject: [redacted]Poprawa zabezpieczeń sieci

Dzień dobry

Nawiązując do rozmowy w sprawie optymalizacji zabezpieczenia sieci LAN i serwerów sugeruję wykonanie kilku, dość czasochłonnych modyfikacji.
Proponuję zmiany zarówno w konfiguracji FortiGate jak również Państwa wewnętrznej infrastruktury LAN.

1. **Przegląd przekierowań portów. Aktualnie jest ich około 50. Stanowi to poważną lukę w bezpieczeństwie.**
Zalecamy możliwie maksymalne ograniczenie tego typu elementów konfiguracji lub ich całkowite wyłączenie, zmieniając przy tym sposób dostępu do wewnętrznych zasobów poprzez VPN.

UTM a bezpieczeństwo

NETIA
netianext

Dzień dobry

W nawiązaniu do rozmowy telefonicznej z Państwa Opiekunem naszych usług, prosimy o ZAWIESZENIE na okres powiedzmy 1 tygodnia usługi Netia Cloud Firewall.
Od czasu, kiedy została aktywowana ta usługa pojawiły się u nas problemy z odbiorem poczty: programy pocztowe odbierają pocztę nieregularnie i często kończą błędem o zerwaniu połączenia.
Szukamy przyczyny tych problemów i na początek chcielibyśmy wykluczyć Wasza usługę.
Prosimy o informację zwrotną, kiedy byłaby taka możliwość, aby móc diagnozować problem.

Pozdrawiam

Pozdrawiam / Regards / Gruesse

[redacted]

From: [redacted]
Sent: Monday[redacted] AM
To: [redacted]
Subject: [redacted] Wirusy z poczcie

Dzień dobry

Nawiązując do rozmowy z Panem [redacted], przesyłam fragment logów z usługi Cloud Firewall.
Dziś w ciągu ostatnich 5 minut wykrytych i zablokowanych zostało około 44 połączeń, z uwagi na wykrycie wirusa w poczcie (protokoły POP3 i IMAP).
Zdarzeń tego typy jest zdecydowanie więcej i występuje w zasadzie ciągle. Blokada niebezpiecznych połączeń jest poprawnym zachowaniem firewalla.

All FortiGate ▾ Last 5 Minutes ▾ [redacted]

Source IP = [redacted] Add Filter

#	▼Date/Time	Device ID	Action	Source	Service	Destination IP	Virus/Botnet
1	09:12:59	FG200[redacted]	blocked	[redacted]	IMAP	[redacted]	W32/BZF!tr
2	09:12:30	FG200[redacted]	blocked	[redacted]	IMAP	[redacted]	W32/BZF!tr
3	09:12:00	FG200[redacted]	blocked	[redacted]	IMAP	[redacted]	W32/BZF!tr
4	09:11:31	FG200[redacted]	blocked	[redacted]	IMAP	[redacted]	W32/BZF!tr
5	09:11:21	FG200[redacted]	blocked	[redacted]	POP3	[redacted]	

UTM a bezpieczeństwo

NETIA
netianext

From: CERT Polska via RT <cert@cert.pl>
Sent: Thursday, June 22, 2023 7:29 PM
To: [redacted]
Subject: [EXT] [CERT.PL #2407698] [PILNE] Powiadomienie CERT Polska/CSIRT NASK w sprawie krytycznej podatności CVE-2023-27997

Szanowni Państwo
jesteśmy zespołem reagowania na incydenty bezpieczeństwa informatycznego CERT Polska. Zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Ponownie kontaktujemy się z Państwem, ponieważ z wykonanego przez nas skanowania wynika, że w Państwa sieci nadal znajdują się hosty z podatną wersją oprogramowania firmy Fortinet. W przypadku, gdy urządzenie to należy do Państwa klientów, prosimy o przekazanie tej wiadomości do odpowiedniego podmiotu.
Podatne instancje znajdują się pod następującymi adresami:
ip:port
[redacted]43
[redacted]443
[redacted]5443
[redacted]443
[redacted]:6443
[redacted]443
[redacted]43
[redacted]4433
[redacted]443
[redacted]443
[redacted]443
[redacted]443
[redacted]2:8443
[redacted]4:444

Nasz zespół otrzymał informację o krytycznej podatności CVE-2023-27997 występującej w usłudze SSL-VPN urządzeń Fortigate z systemem FortiOS w wersjach poniżej 6.0.17, 6.2.15, 6.4.13, 7.0.12 oraz 7.2.5. Jeśli, zgodnie z naszymi informacjami, posiadają Państwo takie urządzenia, zalecamy bezzwłoczne zainstalowanie najnowszych aktualizacji wydanych przez producenta po 8 czerwca 2023, gdyż wspomniana podatność może posłużyć do prób ataków, w tym ataków z użyciem ransomware, na Państwa infrastrukturę.

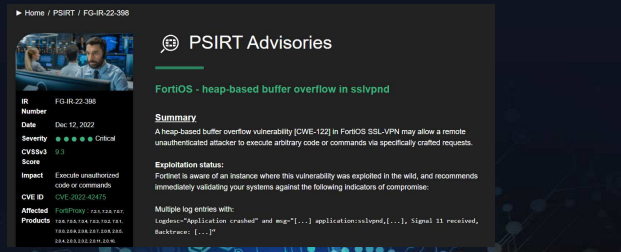
Oficjalny komunikat firmy Fortigate zawierający opis podatności można znaleźć na stronie producenta https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign. Na ten moment wiadomo, że luka umożliwia zdalne wykonywanie kodu bez konieczności dokonywania uwierzytelniania i jest aktywnie wykorzystywana do przeprowadzania ataków typu z wykorzystaniem ransomware.

Prosimy o potwierdzenie otrzymania wiadomości. Jeżeli wskazane w zawiadomieniu hosty zostały już zaktualizowane, również prosimy o informację wraz ze wskazaniem, do jakiej wersji - umożliwi to ograniczenie fałszywych alarmów w przyszłości
W przypadku pytań lub wątpliwości pozostajemy do dyspozycji.

Z poważaniem
Zespół CERT Polska | CSIRT NASK
www.cert.pl

NETIA
netianext

UTM a bezpieczeństwo



UTM a bezpieczeństwo

NETIA
netianext

- „Dziurawy soft”
- Brak wsparcia
- Domyślna konfiguracja
- „Płaska sieć”
- „Przekierowania” portów
- Brak przeglądów konfiguracji
- Brak wiedzy i doświadczenia

NETIA
netianext

O nas

13 inżynierów
(zaczynaliśmy od 2 osób)
24/7

Certyfikaty w Dziale:

Trochę historii…

2017 – powstanie dedykowanego zespołu w Netii

2018 – pierwszy zarządzany przez Netię Fortigate

.

.

.

2023 – ponad 1000 utrzymywanych usług

NETIA
netianext

Trochę historii...

Na początku był....

Fortigate.

NETIA
netianext

Mam **UTM** i czy jestem **bezpieczny?**

NETIA
netianext

FORTINET

EXCLUSIVE NETWORKS