1. **Czy hardware pod SG i XG jest taki sam? Czy można zmieniać soft w obie strony?**

Tak, sprzęt jest taki sam. Różnice dotyczą wyłącznie oprogramowania. Oficjalnie pełna i bez kosztowa migracja z UTM9.x do SF-OS (wraz z licencjami) możliwa jest tylko w jednym kierunku.

FAQs for Sophos UTM customers about the new XG Firewall
https://blogs.sophos.com/2015/11/09/xg-firewall-faq/

2. **Jak jest liczona wydajność? Pasmo czy liczba użytkowników?**

Zależy od podejścia. Do właściwego spozycjonowania urządzenia można użyć obu parametrów. Po szczegóły odsyłamy do Sizing Guidelines dla obu serii produktów:

Sophos SG Series Sizing Guide
https://partnerportal.sophos.com/en-us/medialibrary/PartnerPortal/Files/Tools/SalesGuidance/sophos-sg-series-sizing-guide.pdf?la=en

Sophos XG Series Sizing Guide
https://partnerportal.sophos.com/en-us/medialibrary/PartnerPortal/Files/Tools/SalesGuidance/sophos-xg-series-sizing-guide.PDF?la=en

3. **Czy jest możliwość monitorowania https?**

Tak, SG jak i XG umożliwiają inspekcję ruchu SSL dla ruchu web. Wykorzystywany jest SSL Bridging i podstawianie własnego certyfikatu (rozszywanie ruchu na zasadzie man-in-the-middle)

4. **Czy uruchamianie kolejnych funkcjonalności ma wpływ na wydajność całego rozwiązania? Czyli czy np. po włączeniu WAFa i email protection, network protection jest mniej wydajne?**

Zasoby sprzętowe wykorzystywane przez moduły są współdzielone i uruchamianie kolejnych usług bezpieczeństwa będzie miało wpływ na wydajność:

Wireless Protection: 5% - 10%
Webserver Protection: 10%
URL filter: 10% - 15%
IPS: 40% - 50%

Szczegóły na ten temat można znaleźć w dokumentach Sizing Guide (patrz linki powyżej)

5. **Jak dokładnie działa funkcjonalność Sandstorm. Na jakiej podstawie wybierane są pliki. Jak nie ma sygnatur to skąd wiadomo, ze plik powinien być wybrany?**

   Plik po przejściu przez standardowe mechanizmy takie jak fitlr Web, AV, Live Protect, IPS poddawany jest dodatkowej analizie. Najpierw wysyłany jest tylko hash. W przypadku jeśli w skali globalnej plik ten nigdy nie był jeszcze analizowany, wysyłana jest jego kopia. Następnie plik uruchamiany jest w kontrolowanym i odizolowanym środowisku by sprawdzić jego zachowanie. Po przeprowadzeniu badania powstają hash, ocena i raport a plik jest usuwany. Więcej szczegółów dostępnych na stronie:

   https://www.sophos.com/lp/sandstorm.aspx

6. **Czy uruchomienie Sandstorm powoduje duże opóźnienia podczas przeglądania stron czy nie ma to znaczenia?**

Opóźnienia w przeglądaniu stron nie będą zauważalne. Opóźnienie w dostarczeniu pobieranych plików może pojawić się tylko w przypadku gdy plik zostanie odesłany do inspekcji. Użytkownik zostanie o tym poinformowany w oknie przeglądarki. Analiza takiego pliku zajmuje około 120 sekund.

7. **Jaka strategia w przypadku zaszyfrowanych plikow, word z haslem, 7z z hasłem**

Pliki szyfrowane nie będą mogły zostać rozpakowane vide nie podlegają inspekcji.

8. **Czy tyczy się to plików w mailach czy zapisanych na dysku również?**

Sandstorm działając na UTM, Web Gateway czy Email Gateway analizuje jedynie pliki przesyłane pocztą i/lub przez web (w zależności od rozwiązania)

9. **Pliki Word też są wysyłane do Sophos Sandstorm do analizy?**

Tak. Sandstorm analizuje ponad 20 typów plików (w tym (*.doc, *.docx, *.docm, *.rtf)

10. **Czy można zarządzać heartbeat bez udziału chmury (instalacja on-premise)?**

Nie. Funkcjonalność Sophos Secure Heartbeat wymaga Sophos Central (do niedawna Sophos Cloud)

Sophos Security Hearbeat
https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-security-heartbeat_dsna.pdf?la=en

11. Różnice pomiędzy Astaro a Cyberoam

Aktualne różnice między SF-OS a UTM dostępne pod adresem:

https://partnerportal.sophos.com/en-us/medialibrary/PartnerPortal/Files/Tools/Datasheets/Unified/sophos-sf-os-vs-utm-feature-list.pdf?la=en

12. Czy wspierany jest w XG protokół IMAP?

Tak. Pełna lista funkcjonalności dostępna pod adresem:

https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosxgfirewallflna.pdf?la=en

13. Do Heartbeat wymagany jest klient?

Tak. Wymagany jest Sophos Cloud Endpoint Protection Advanced lub Sophos Cloud Enduser Protection

https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-security-heartbeat_dsna.pdf?la=en