O ile zapewnienie bezpieczeństwa od strony Internetu jest dzisiaj czymś zupełnie oczywistym o tyle organizacje często zapominają o ochronie sieci wewnętrznej. Możliwości współczesnych urządzeń sieciowych, czyli zarówno punktów dostępowych Wi-Fi jak i przełączników, umożliwiają wdrożenie mechanizmów mogących zautomatyzować proces segmentacji sieci i ograniczania uprawnień do aplikacji i usług

Rola systemów Network Access Control

Do uruchomienia uwierzytelniania w sieci wewnętrznej wystarczy zintegrowanie posiadanych urządzeń sieciowych z serwerem RADIUS: może to być bezpłatny serwer *FreeRADIUS* lub, w przypadku gdy w firmie uruchomiona jest usługa *Microsoft Active Directory*, serwer z zainstalowaną rolą *Network Policy Server*. Niezależnie od wybranego rozwiązania pojawiają się problemy, które mogą bardzo utrudnić lub wręcz uniemożliwić wdrożenie kontroli dostępu:

- Ujednolicone, spójne zarządzanie rolami użytkowników i urządzeń końcowych
- Ogrom manualnej pracy związanej z konfiguracją i późniejszym zarządzaniem zmianami w sieci
- Brak lub bardzo ograniczone możliwości integracji z posiadanymi rozwiązaniami firm trzecich.

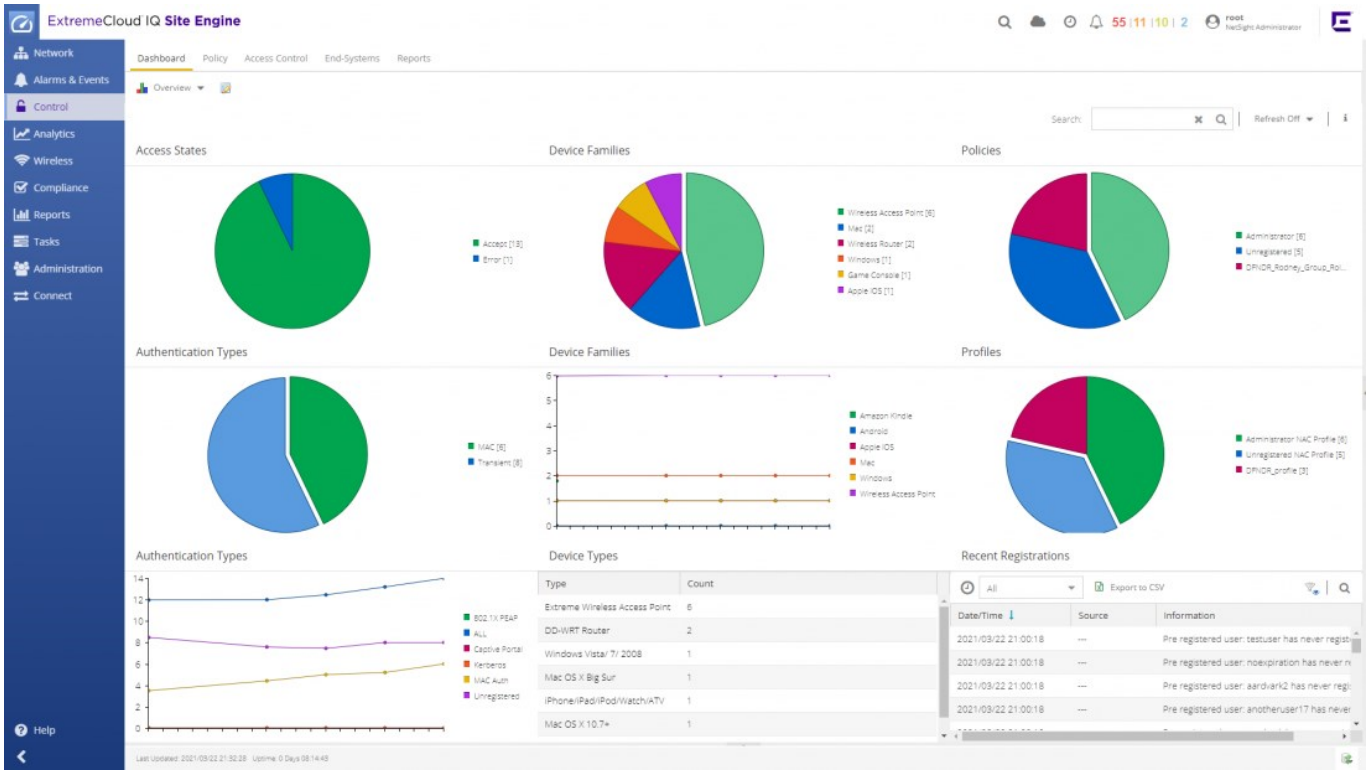
Naprzeciw tym niedogodnościom powstały Systemy Kontroli Dostępu do Sieci czyli tzw. NAC (Network Access Control)

Możliwości Extreme Control NAC

Jednym z wiodących rozwiązań NAC na rynku jest system Extreme Control oferujący m.in.:

- Dostęp do sieci w oparciu o centralnie konfigurowane Role w ramach modułu Extreme Policy
- Bezpieczny dostęp gościnny oraz kontrolowany dostęp dla urządzeń prywatnych pracowników (tzw. dostęp BYOD – *Bring Your Own Device*)
- Współpracę z dowolnymi zgodnymi urządzeniami sieciowymi LAN/WLAN
- Integrację z Active Directory/openLDAP
- Integrację z firewallami NGFW (Check Point, Palo Alto, Fortinet), oraz SIEM, CMDB i systemami EMM/MDM (VMware AirWatch, Citrix XenMobile, MobileIron, Microsoft Intune) i in. dzięki modułowi Extreme Connect
- Integrację z rozwiązaniem Extreme Analytics w cenie rozwiązania

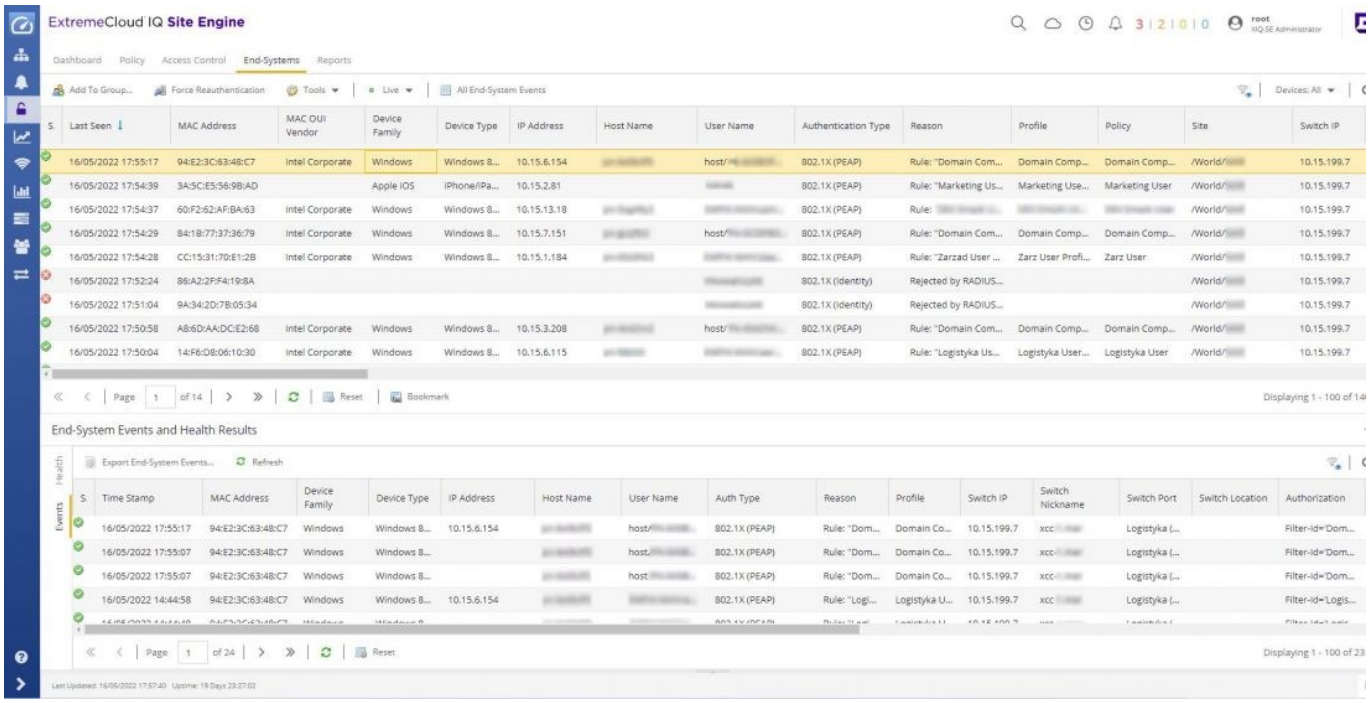
Extreme Control może zostać zintegrowane z dowolnym przełącznikiem sieciowym lub systemem WLAN obsługującym protokół RADIUS oraz uwierzytelnianie użytkowników metodami 802.1x i MAC. Ponadto system prawidłowo obsługuje niestandardowe atrybuty RADIUS VSA oraz posiada zaimplementowane biblioteki SNMP MIB wiodących producentów urządzeń sieciowych na rynku, dzięki którym system może mieć szerszy dostęp do informacji i funkcji niedostępnych w ramach protokołu RADIUS.



Global One jako wieloletni integrator systemów Extreme NAC w Polsce posiada praktyczne doświadczenie w integracji z przełącznikami firm trzecich (m.in.: Cisco, Alcatel, Huawei)

Architektura rozwiązania

Extreme Control opiera się na jednej lub większej liczbie dedykowanych maszyn wirtualnych realizujących funkcje NAC (*NAC Engine*) oraz konsoli zarządzania **XIQ-Site Engine** służącej do zarządzania i monitorowania uwierzytelnianych urządzeń końcowych w sieci.



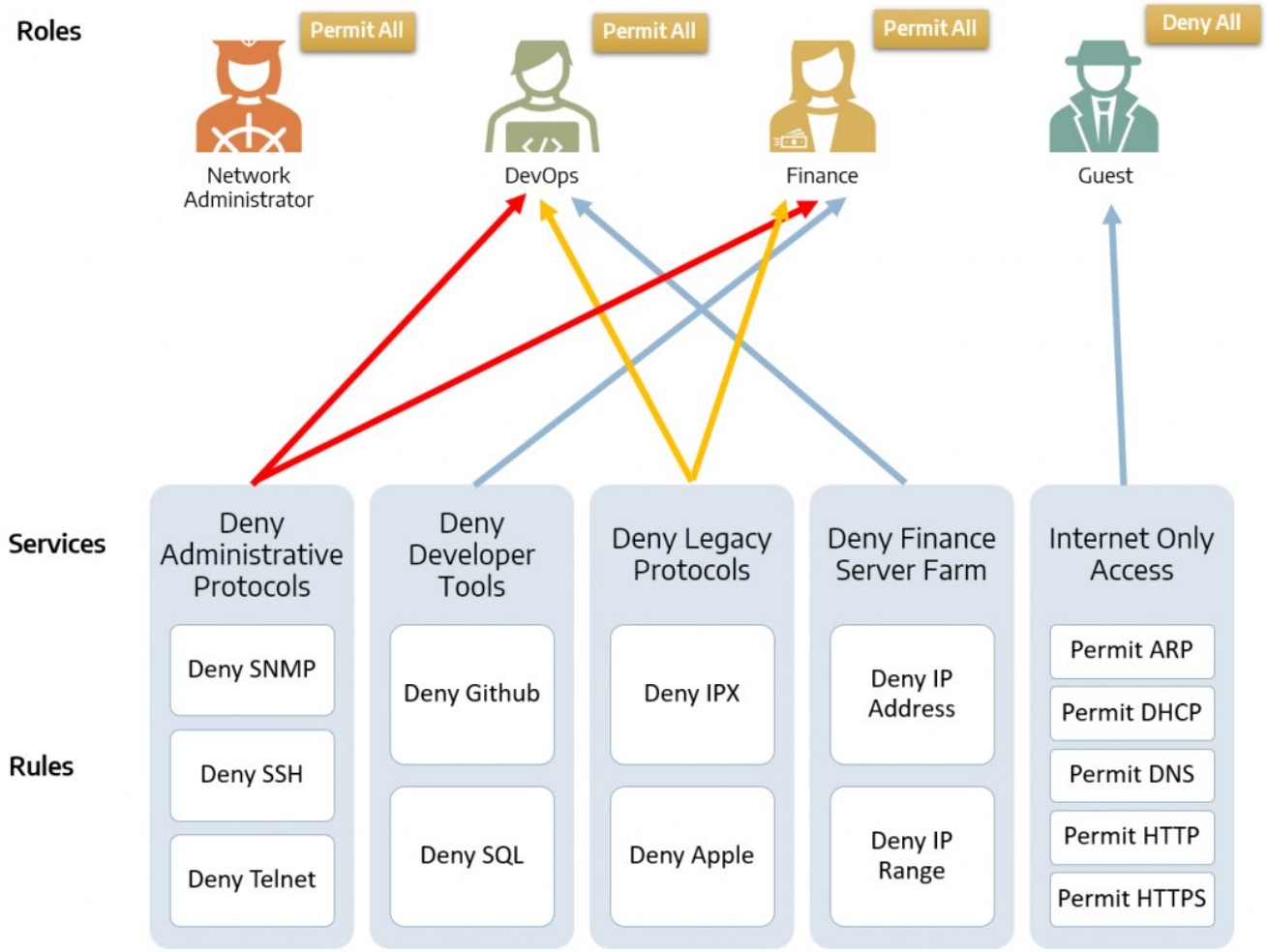
Podgląd w czasie rzeczywistym wszystkich urządzeń końcowych w sieci z poziomu systemu NAC.

Extreme Policy

Role użytkowników i urządzeń mających za zadanie odzwierciedlenie faktycznych funkcji użytkowników w organizacji (Administrator, Księgowy, Sekretarka, Dyrektor, Gość itp.) czy też urządzeń (Komputer, Telefon IP, Drukarka) tworzone są w module Extreme Policy, będącym częścią konsoli zarządzania XIQ-Site Engine. Każda Rola zawiera szereg tzw. Usług składających się z listy szczegółowo zdefiniowanych Reguł egzekwowanych bezpośrednio na poziomie portu przełącznika czy Access Pointa.

Role posiadają ponadto zdefiniowany VLAN użytkownika (w tym VLAN przekazywany zgodnie z RFC 3580) czy opcjonalne atrybuty QoS (w zależności od obsługiwanych funkcji przez dane urządzenie sieciowe).

Po skonfigurowaniu Roli te są następnie tłumaczone przez cały system na zestaw reguł ACL wykorzystywanych do autoryzacji urządzeń uwierzytelnianych przez NAC.



Oprócz urządzeń Extreme moduł Extreme Policy obsługuje również przełączniki Cisco i HPE.

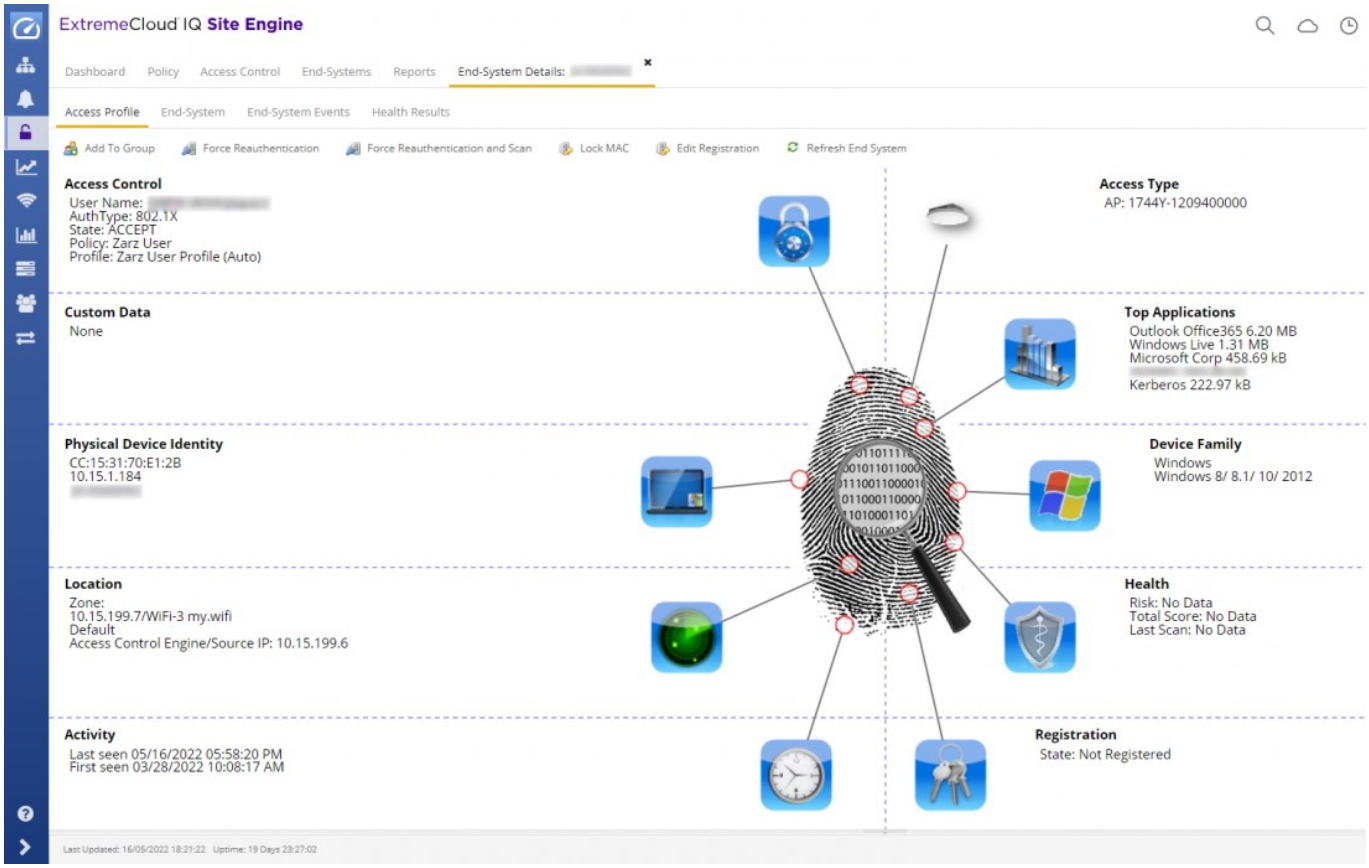
Dzięki Extreme Policy aktualizacja uprawnień dla grup użytkowników czy urządzeń w całej sieci może być prowadzona bez jakiegokolwiek kontaktu administratorów z CLI urządzeń sieciowych

Działanie Extreme Control

Działanie Extreme Control opera się na sprawdzaniu listy Reguł uwzględniających:

- Metodę uwierzytelnienia (802.11x, MAC, Captive Portal)
- Grupę użytkownika (np. grupa Active Directory)
- Profil urządzenia – system rozpoznaje czy z siecią łączy się smartphone Android/iPhone czy też komputer Windows/Mac
- Grupę urządzenia – członkostwo na podstawie adresu MAC, producenta czy nazwy DNS
- Lokalizację rozumianą jako konkretny przełącznik, port sieciowy, AP czy też nazwa sieci Wi-Fi
- Harmonogram zdefiniowany jako konkretne dni tygodnia i godziny

Gdy uwierzytelniane urządzenie końcowe trafia do danej Reguły NAC następuje przesłanie odpowiedniej autoryzacji wynikającej wprost z uprzednio skonfigurowanej Roli.

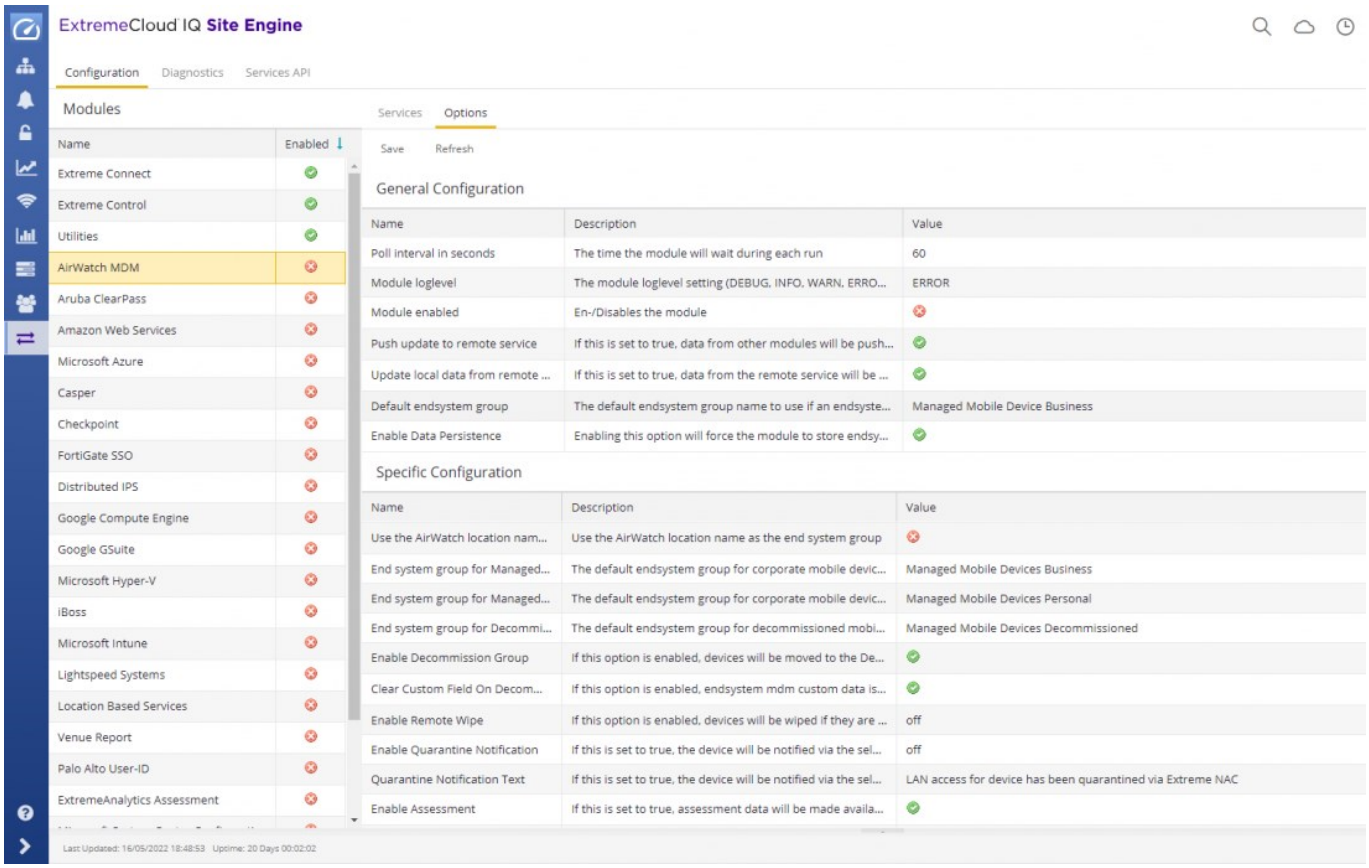


Prezentacja danych zgromadzonych na temat urządzenia końcowego przez system NAC.

Extreme Connect

Extreme Connect jest to moduł konsoli zarządzania XIQ-Site Engine posiadający zestaw gotowych wtyczek do integracji z szeroką listą rozwiązań firm trzecich. Najważniejsze integracje pod kątem funkcjonalności NAC to m.in.: EMM/MDM: VMware AirWatch, Citrix XenMobile, MobileIron, Microsoft Intune czy NGFW: Checkpoint, Palo Alto, Fortinet.
Dzięki przygotowanym przez producenta integracjom z zewnętrznymi systemami bezpieczeństwa możliwe jest ograniczanie lub wręcz całkowite zablokowanie dostępu do sieci przez Extreme Control dla urządzeń:

- Niespełniających podstawowych kryteriów ochrony (np. włączony antywirus, zainstalowane poprawki systemowe, włączony firewall)
- Określonych przez zewnętrzne systemy bezpieczeństwa jako skompromitowane lub niebezpieczne
- Niezarejestrowanych lub obcych



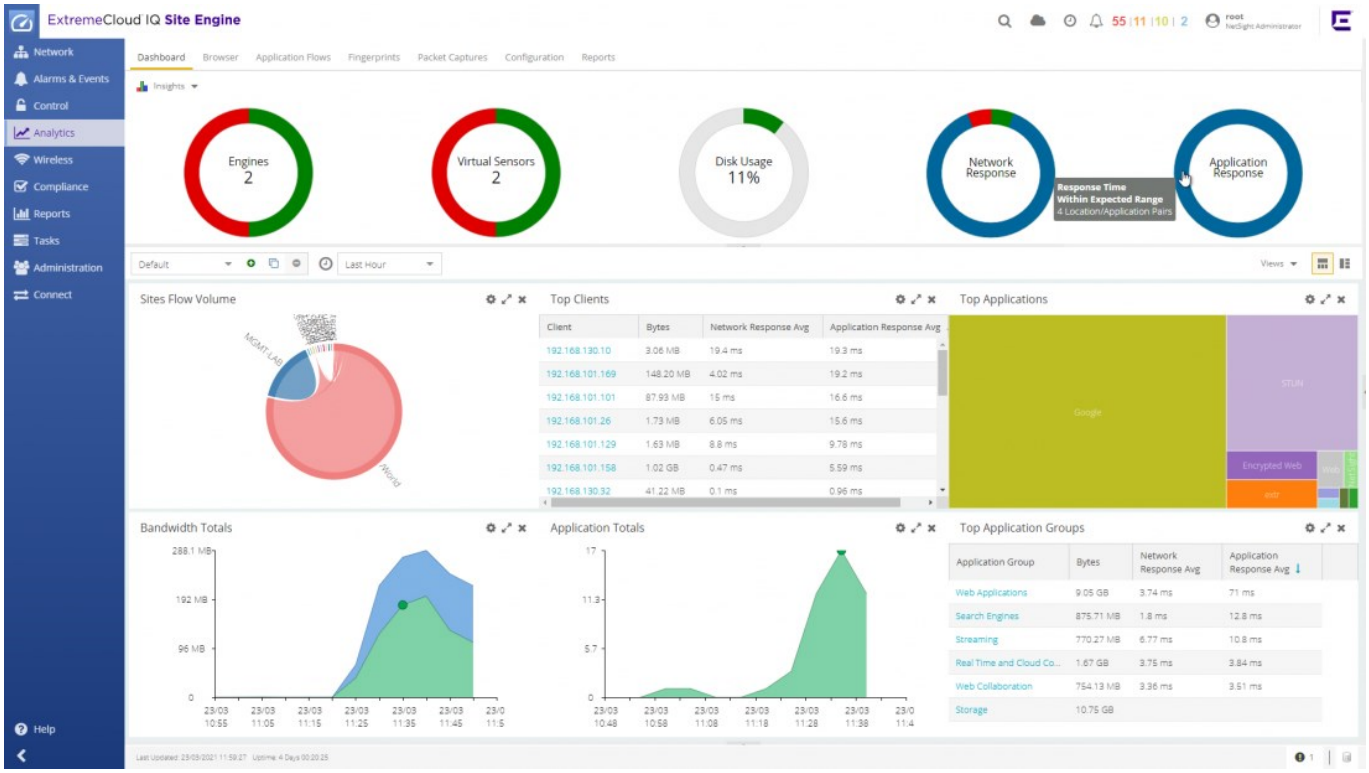
Dzięki obsłudze RFC 3576 możliwa jest dynamiczna zmiana Roli uwierzytelnionego urządzenia w odpowiedzi na wykryte zagrożenie i wykorzystanie w ten sposób możliwości zintegrowanych z NAC systemów do ochrony sieci wewnętrznej organizacji.

Extreme Analytics

Extreme Analytics jest rozwiązaniem Business Intelligence analizującym ruch sieciowy generowany przez aplikacje użytkowników. Do listy praktycznych przykładów wykorzystania Analytics do rozwiązywania rzeczywistych problemów biznesowych można zaliczyć:

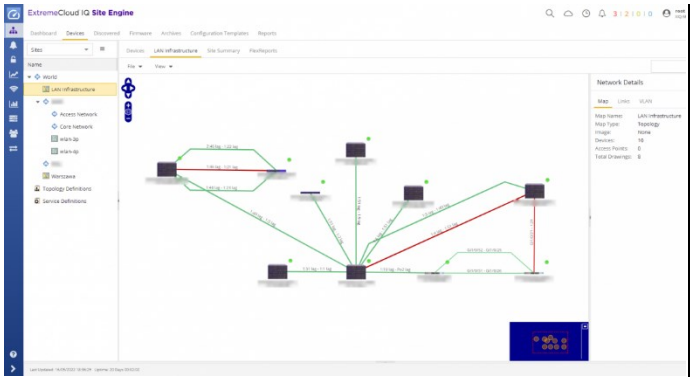
- Podejmowanie decyzji o potrzebie przeniesienia aplikacji do innej lokalizacji
- Wykrywanie wolno działających aplikacji
- Określenie źródła problemów z wydajnością poprzez wskazanie czy dotyczy on sieci, klienta, serwera, czy np. pamięci masowej
- Wykrywanie złośliwych lub niedozwolonych aplikacji
- Określenie skali wdrożenia aplikacji w organizacji
- Monitorowanie czy użytkownicy nie wykorzystują nielicencjonowanego (pirackiego) oprogramowania

Extreme Analytics składa się z serwera Extreme Analytics (Analytics Engine) analizującego statystyki NetFlow i fragment kopii ruchu sieciowego przekazywanego ze zgodnych urządzeń i aplikacji Extreme. Rozwiązanie, podobnie jak Extreme Control, jest zarządzane z poziomu konsoli zarządzania XIQ-Site Engine oraz dodatkowo uzupełnia gromadzone dane o urządzeń końcowych w sieci przez system NAC.



Pozostałe moduły XIQ-Site Engine

XIQ-Site Engine posiada dodatkowe moduły związane z zarządzaniem podłączonymi urządzeniami sieciowymi Extreme oraz innych producentów.

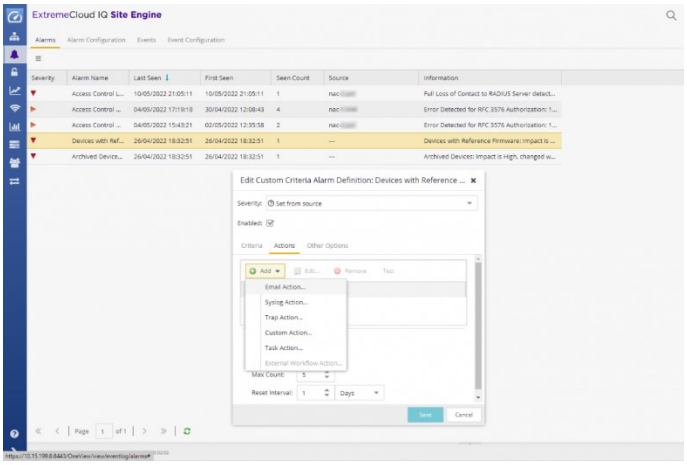


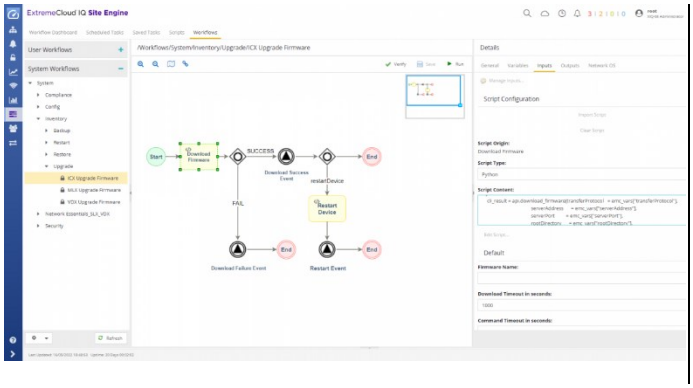
Network

Moduł Network posiada gotowe narzędzia do tworzenia kopii zapasowych konfiguracji urządzeń wiodących producentów oraz wygodne aktualizowanie ich oprogramowania. Ponadto obsługuje funkcję tworzenia interaktywnych map sieci z wykorzystaniem protokołów CDP, EDP i LLDP.

Alarms & Events

Moduł alarmowania umożliwia tworzenie powiadomień dla administratorów i zewnętrznych systemów. Posiada proste w konfiguracji reguły bazujące na słowach kluczowych i wyrażeniach regularnych.





Tasks

Moduł zadań służy do automatyzacji procedur administracyjnych w formie tzw. Workflow. Każdy Workflow składa się z zestawu instrukcji, reprezentowanych w formie przejrzystego schematu blokowego, mogących zawierać zarówno zwykłe komendy przekazywane do urządzenia jak również skrypt w języku TCL/Python.

Zapraszamy do kontaktu z naszym biurem w celu przedstawienia oferty lub organizacji spotkania.