GRANDMETRIC
STAY CONNECTED.

Cisco Partner

OKIEM INŻYNIERA

Cisco ISE

GRANDMETRIC
STAY CONNECTED.

Spis treści

Wstęp

Utrata strategicznych plików, wyciek danych osobowych, kradzież dokumentacji czy raportów, szpiegostwo przemysłowe. Wraz ze wzrostem znaczenia i wartości in- formacji, rośnie liczba zagrożeń.

Szacuje się, że do 2025 roku **straty spowodowane naruszeniami bezpieczeństwa** na całym świecie osiągną nawet **10,5 bilionów dolarów**1.

Cyberataki nie dotyczą już wyłącznie największych graczy na rynku. Chcąc ograniczyć ryzyko, a jednocześnie zdobyć łatwy łup, **hackerzy atakują** przede wszystkim średnie i małe **organizacje, które nie przykładają odpowiedniej wagi do ochrony swoich zasobów.** Takie działanie to **małe ryzyko i pewny zysk.**

Czy standardy bezpieczeństwa są ważne tylko z naszej perspektywy? Według danych raportu State of Security 2022, brak wystarczającego poziomu zabezpieczeń **może wpłynąć negatywnie** na **pozyskiwanie nowych klientów** lub nawet w ostatniej chwili **powstrzymać** klienta **przed podpisaniem umowy.**

Na coraz bardziej wyszukane metody przestępców starają się odpowiedzieć coraz to nowe narzędzia mające zapewnić bezpieczeństwo sieci, a sama **branża cyberbezpieczeństwa jest jedną z najszybciej rosnących gałęzi przemysłu technologicznego.** Głównym **katalizatorem zmian**, które zapoczątkowały gwałtowny rozwój tego obszaru jest pandemia **COVID-19** i jej następstwa. Nie bez znaczenia jest również to, co nazywa się czwartą rewolucją przemysłową lub **przemysłem 4.0** – powszechną digitalizację usług i produkcji. Zaczęły pojawiać się całe działy odpowiedzialne za ochronę organizacji, a na najwyższych szczeblach, oprócz dyrektorów technologicznych, stanęli ci od zabezpieczeń. Swoją cegiełkę dołożyła też… chciwość przestępców i ryzyko związane z potencjalnym atakiem. **Również małe firmy decydują się na przynajmniej podstawowe zabezpieczenia**, ponieważ nawet pomniejszony zysk **to szansa na przetrwanie** wobec zbyt wygórowanych żądań przestępców.

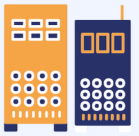
Wzrost świadomości cyberbezpieczeństwa

Praca zdalna

Potrzeba zdalnego dostępu do sieci

Cyfryzacja procesów

IoT



Zetabajty zbieranych i przechowywanych danych

1 "2022 Official Cybercrime Report, sponsored by eSentire.

Czym jest system NAC?

Mogłoby się wydawać, że wykorzystując komputery firmowe jedynie do celów służbowych, blokując niebezpieczne strony i inwestując w firewall, nic nam nie grozi. Zagrożenie jednak nie musi wcale pochodzić bezpośrednio z internetu. **Naruszeniem bezpieczeństwa jest każde zalogowanie się nieuprawnionych urządzeń do firmowej sieci.** To na przykład prywatny tablet niczego nie spodziewającego się pracownika. Tablet, na którym podłączony do Wi-Fi gra w Tetrisa i może nie mieć wystarczającej ochrony – otwierając tym samym drzwi przestępcy. To także laptop przedstawicielki handlowej, która w sali konferencyjnej podpięła się do kabla Ethernet, by włączyć prezentację. Przedstawicielka... wcale nie musi być przedstawicielką. Może okazać się faktyczną hackerką, która w kilka chwil wyciągnie dane osobowe kadry, kontakty biznesowe czy informacje pozwalające zdobyć przewagę konkurencyjną.

Narzędzia ochrony sieci wewnętrznej **nie** zawsze **muszą być skomplikowane**, by zapewnić bezpieczeństwo. Czasami nawet **proste rozwiązania**, takie **jak system NAC**, są w stanie powstrzymać zagrożenie. Jak to działa?

Network Access Control (NAC) to system pozwalający na rozpoznanie, weryfikację, uwierzytelnienie i zebranie informacji o urządzeniach logujących się do sieci. Dzięki NAC wiadomo kto, gdzie i kiedy nawiązał połączenie. Na podstawie określonych kryteriów narzędzie może zaakceptować dane urządzenie lub odmówić mu dostępu. Niezależnie od tego czy łączymy się przez Wi-Fi czy „po kablu”, NAC jest pierwszym stykiem urządzenia z siecią.

NAC można porównać do recepcjonistki lub strażnika przy wejściu do budynku. Jeśli mamy przepustkę – wejdziemy od razu. Jeśli nie, sprawdzą naszą tożsamość, ustalą cel wizyty, zweryfikują, czy jesteśmy umówieni, skierują nas w odpowiednie miejsce i odnotują wejście w dzienniku. Jeśli to konieczne, mogą nam nawet odmówić wstępu do dalszej części budynku.

– Karol Goliszewski, Consulting Engineer

Zaawansowane narzędzia kontroli dostępu pozwalają na:

- Wzmocnienie bezpieczeństwa poprzez identyfikację i kontrolę dostępu urządzeń do sieci organizacji.
- Zarządzanie dostępem do zasobów pomiędzy działami.
- Zarządzanie dostępem dla gości np. poprzez dedykowany Captive Portal, generowanie hasła jednorazowego lub przeniesienie na inną sieć. To dobrze znana podróżującym strona logowania do hotelowego lub lotniskowego Wi-Fi.
- Sprawdzenie i ocenę poziomu zabezpieczeń urządzenia chcącego uzyskać połączenie z siecią.
- Kontrolę urządzeń mających dostęp do sieci i możliwość ich odłączenia.
- Tworzenie szczegółowych raportów logowania.

Dlaczego firmy wdrażają NAC?2

- Przystosowanie sieci pod certyfikaty bezpieczeństwa lub chęć podniesienia poziomu zabezpieczeń.
- Integracja z innymi zabezpieczeniami.
- Zagrożenie ze względu na dużą liczbę logowań zewnętrznych urządzeń.
- Stworzenie środowiska pozwalającego na kwarantannę urządzeń bez zakłócania funkcjonowania firmy.

Skalowalność i uniwersalność narzędzia pozwala na **zastosowanie go w organizacji każdej wielkości**, niezależnie od tego, czy zatrudnia 20 czy 20000 osób. Nie gra roli również gałąź gospodarki, w której funkcjonuje. **Wdrożenie warto jednak szczególnie rozważyć w miejscach, gdzie często przyjmowani są goście, przetwarzających dane wrażliwe, czy nawet zamkniętych obiektach, gdzie przechowywane są szczególne cenne informacje lub gdzie wiele urządzeń połączonych jest w IoT.**

NAC to podstawa każdego systemu ochrony i powinien być pierwszym wyborem przy zabezpieczaniu sieci. Praktyka pokazuje jednak, że wdrażany jest dopiero na późniejszych etapach co sprawia, że czasem pomimo wysokiej klasy pozostałych narzędzi, dostęp może uzyskać każdy, kto kliknie przycisk Połącz. **Skarbiec jest tak bezpieczny, jak chroniące go drzwi**, a jeśli te są otwarte na oścież, łatwo splądrować jego zawartość.

System NAC jest odpowiedzią na potrzebę kontroli urządzeń, które podłączają się do danej sieci, aby robiły to w sposób ułożony, scentralizowany i zgodny z polityką bezpieczeństwa.

– Marcin Biały, Advisory Architect

2 “What Is Network Access Control?, Chiradeep BasuMallick

Podstawy działania NAC

Systemy NAC co do zasady działają w podobny sposób, ponieważ opierają się na ustandaryzowanym na całym świecie protokole RADIUS wraz z rozszerzeniami, a samo uwierzytelnianie i autoryzacja wspierana jest m.in. przez standard IEEE 802.1x. Systemy mogą się jednak różnić w zależności od tego, na jakim etapie urządzenie jest kontrolowane. Posługując się znaną już analogią – czy jest to strażnik przy bramie, czy recepcjonistka już wewnątrz budynku.

Czego potrzebujemy do tego, żeby realizować uwierzytelnianie w oparciu o protokół 802.1x? Końcówka musi zawierać w sobie oprogramowanie, które nazywa się suplikantem i umożliwia działanie protokołu 802.1x. NAC potrzebuje oczywiście urządzenia sieciowego typu przełącznik czy kontroler sieci Wi-Fi, który wspiera 802.1x, ale po stronie klienta, czyli po stronie urządzenia, niezbędny jest suplikant. Nasze komputery z MacOS, Linuxem czy Windows, posiadają suplikanta zaszyte- go w systemach operacyjnych i są zdolne do realizacji komunikacji poprzez protokół 802.1x. Natomiast wiele innych urządzeń typu czujniki, drobne IoT, urządzenia automatyki przemysłowej, takiego suplikanta nie posiada. Wówczas musimy się opierać kontrolę dostępu wyłącznie o adres MAC, a urządzenia ręcznie dodać do bazy systemu NAC.

System NAC a serwer Radius

W swojej podstawie, NAC to serwer RADIUS, ale rozszerzony o mnóstwo funkcjo- nalności wspierających bezpieczeństwo. To nie jest już zerojedynkowa ochrona polegająca na podejmowaniu decyzji: „wpuszczam lub nie wpuszczam do sieci”. To zautomatyzowana platforma reagująca na szereg występujących równole- gle czynników.

Jakie korzyści daje NAC w porównaniu z Radiusem na etapie wdrożenia w sporej, bardzo różnorodnej sieci? Przyjrzyjmy się temu w formie tabeli. Korzyści jest dużo więcej, w zależności od konkretnego produktu. Poniższa tabela zawiera te z nich, które jednoznacznie wskazują, czym tak naprawdę jest system klasy NAC.

Korzyści	System klasy NAC	Prosty serwer RADIUS
Uwierzytelnianie z wykorzystaniem protokołu 802.1x (login i hasło lub certyfikat)	✓	✓
Uwierzytelnianie w oparciu o adres MAC	✓	✓
Bieżące raportowanie statusu uwierzytelniania (kto i kiedy się uwierzytelnił, bądź kto i kiedy został odrzucony)	✓	✓
Możliwość ustawiania dodatkowych parametrów w politykach, od których zależy rezultat, czyli dostęp do określonego VLAN-u lub odrzucenie hosta z sieci, takich jak: • data i godzina logowania do sieci, • grupa w AD, do której przynależy host lub użytkownik, • grupa adresów MAC, do której należy dane urządzenie • port na przełączniku, do którego urządzenie jest podłączane, lub sieć WiFi, do której się łączy, • sprawdzenie, czy dany komputer ma odpowiednią kondycję (czy jest aktywny firewall systemowy, aktualny program antymalware, aktualny system operacyjny, etc.), • dostęp do określonej podsieci na podstawie klasyfikacji końcówki (jeżeli producent urządzenia to X = VLAN 10, jeżeli producent Y = VLAN 20, etc.), • korelacja powiązań komputer=pracownik (jeżeli na laptopie X zaloguje się Jan Kowalski = przydziel VLAN 10, jeżeli natomiast zaloguje się ktokolwiek inny = przydziel VLAN gościnny lub odrzuć połączenie), • ... i wiele, wiele, wiele innych	✓	✗
Dostęp gościnny realizowany w oparciu o Captive Portal (dostępy sponsorowane, logowanie powiązane z zewnętrznymi serwisami, np. Facebook, Google, etc., SMS-kody dostępowe z hasłem jendorazowym, etc.)	✓	✗
Automatyzacja zdarzeń (przykłady: jeżeli komputer raportuje status „zainfekowany” – odłącz go od VLAN-u produkcyjnego, przydziel VLAN kwarantanny i poinformuj administratora; jeżeli dany komputer podłączył się do innego przełącznika niż zwykle – poinformuj administratora; jeżeli na danym porcie przełącznika wykonano dziesięć lub więcej nieudanych prób podłączenia się do sieci – zablokuj port i poinformuj administratora), etc.	✓	✗
Integracje z systemami zewnętrznymi, umożliwiające rozszerzenie ochrony wykorzystywanych w organizacji syste- mów – np. integracja z firewallem (log dotyczący ataku hackerskiego na komputer wysłany z firewallowej sondy IPS może sprawić, by NAC odłączył ten komputer od sieci i powiadomił administratora, etc.	✓	✗
Serwer TACACS+ Dodatkową funkcją dla niektórych systemów NAC jest Admin Access, który działa na podstawie protokołu TACACS+. Jest bezpieczniejszy niż standardowe narzędzia i pozwala na przyznawanie uprawnień do urządzeń sieciowych. Dany administrator otrzymuje dostęp nie tylko do określonych urządzeń, ale też do danego typu komend. Daje też możliwość sprawdzenia, kto i na jakim urządzeniu wpisał daną komendę, lub ogranicza ich wykorzystanie.	✓	✗

Korzyści	System klasy NAC	Prosty serwer RADIUS
Moduły ułatwiające administrację siecią (serwery DHCP, system IPAM, kolektor syslog, etc.)	✓	✗
Zaawansowane raportowanie zdarzeń związanych z próbą dostępu do sieci (łatwość wytypowania i wskazania miejsc, w których dochodzi do prób sforsowania sieci z dokładnością do pojedynczego portu na przełączniku lub konkretnego access pointa)	✓	✗
Dodatkowe moduły wzbogacające funkcjonalność bądź ułatwiające administrację dostępem do sieci: autokonfiguratory urządzeń końcowych (należy pamiętać, że uwierzytelnianie 802.1x wymaga także skonfigurowania suplikanta na urządzeniach końcowych! O ile pewną ilość urządzeń wspierających ten protokół można skonfigurować ręcznie, o tyle ich wielkoskalowa konfiguracja może być bardzo czasochłonna. Systemy klasy NAC często są wyposażone w oprogramowanie, które sprowadza konfigurację urządzenia końcowego do pojedynczych kliknięć), rozszerzenia powłok systemów operacyjnych (np. aplikacja na system Windows umożliwiająca zmianę VLAN-u na określonym porcie danego przełącznika jednym kliknięciem, etc.)	✓	✗

Rozwiązania NAC - Cisco ISE

Myśląc o NAC albo szerzej, o cyberbezpieczeństwie i transformacji cyfrowej, Cisco jest jedną z pierwszych nazw, które przychodzą do głowy. Pochodząca ze Stanów Zjednoczonych organizacja jest jednym z przodujących graczy na rynku rozwiązań IT.

Cisco Identity Service Engine opiera się na zasadzie Zero Trust, która mówi o domyślnym braku zaufania względem wszystkich urządzeń i użytkowników podłączających się do sieci. ISE weryfikuje urządzenie, uwierzytelniając je, robiąc opcjonalny posture assessment, czyli sprawdzenie stanu stacji, a następnie przydziela konkretne zestawy uprawnień w dostępie do sieci. To profesjonalnie przygotowany NAC, nieustannie rozwijany pozwalający na uzyskanie takich funkcji jak AAA, guest access, profiling, Posture, pxGRid (protokół “ekosystemu” rozwiązań wymieniających ze sobą informację o zdarzeniach w sieci). Weryfikuje urządzenie końcowe w trakcie podłączenia do sieci, ocenia je i powstrzymuje potencjalne zagrożenie, zanim dostanie się do sieci.

Rozpoznawalność, renoma i powszechne zaufanie to gwarancja jakości, jednak należy pamiętać, że za ja- kość się płaci. Odpowiedzią na wyzwanie i cenę jest jednak modułowość rozwiązania, która zakłada, że użytkownik płaci jedynie za te funkcjonalności, które wykorzystuje.

Ogólne wrażenia i zastosowanie

Cisco ISE jest zaawansowanym rozwiązaniem NAC, które skaluje się, pozwalając na wspieranie małych, ale też globalnych organizacji funkcjonujących we wszystkich regionach świata. Jego możliwości wykraczają znacznie poza wsparcie mechanizmów 802.1x, ponieważ dostępne są takie funkcjonalności jak rozbudowany guest access, posture assessment, profiling, Azure AD integration, komunikacja pxGrid, integracja z systemami MDM (Mobile Device Management), czy SGT (Security Group Tag). Podobnie jak w większości przypadków, nie wymaga już infrastruktury on-premise i może funkcjonować całkowicie zdalnie.

ISE poza podstawowymi funkcjami NAC, potrafi profilować np. system operacyjny czy szczegóły urządzenia, a także dokonać sprawdzenia kondycji stacji (posture). Na tej podstawie można ustalić bardziej granularne polityki bezpieczeństwa i uzależnić je od typu urządzenia, a podłączając urządzenia do sieci zyskać pewność ich zgodności z polityką bezpieczeństwa.

– Marcin Biały, Advisory Architect

Wdrożenie i konfiguracja

Obszerna dokumentacja, rozbudowana społeczność i łatwość obsługi sprawiają, że wprawny administrator jest w stanie zaimplementować i skonfigurować rozwiązanie we własnym zakresie.

Z pomocy zewnętrznych partnerów korzysta się najczęściej przy większych sieciach, gdzie mamy do czynienia ze skomplikowaną architekturą, urządzeniami różnych producentów czy ogólnym nieuporządkowaniem. Doświadczenie, znajomość scenariuszy i świadomość ryzyk zapewniają wtedy jakość wdrożenia i pozwalają uniknąć niespodzianek.

Ustalanie reguł w Cisco ISE jest bardzo granularne i daje ogromne możliwości konfiguracji.

Pomocna jest też wersja testowa, gdzie **przez 90 dni** można korzystać bez opłat z oprogramowania w najwyższej wersji, samemu przejść przez wszystkie funkcje i zdecydować, które z nich rzeczywiście są potrzebne.

Niezawodność

Niezależnie od systemu, NAC będzie tak stabilny jak serwer, na którym pracuje. Największa odpowiedzialność za dostarczenie odpowiedniej infrastruktury leży po stronie organizacji, w której wdrażane jest narzędzie. Jeśli będzie niewystarczające, nawet najlepszy system może się zawiesić lub, w skrajnym przypadku, wyłączyć. Producenci określają na swoich stronach internetowych minimalne wymagania dla każdego rozwiązania.

Wykorzystanie maszyn wirtualnych i możliwość skalowania sprawiają, że system jest stabilny i redundantny.

Integracja

Stworzony z myślą o łatwej integracji, posiada otwarte API i protokół pxGrid – protokół, który potrafi wymieniać informacje o podłączonym użytkowniku/urządzeniu np. z firewallem różnych producentów, o ile go obsługują. Pozwala to na łatwiejszą konfigurację i ustawianie reguł, ponieważ możliwe staje się rozpoznawanie użytkowników po innych parametrach niż adres IP np. nazwie użytkownika lub grupie domenowej, dzięki czemu użytkownik niezależnie od lokalizacji i adresacji IP, w której się znajduje, otrzyma taki sam zestaw uprawnień na urządzeniach firewall prowadzących do żądanych zasobów.

Dla urządzeń mobilnych świetnie działa z systemem MDM.

Cisco ISE zostało stworzone jako serce całego ekosystemu zabezpieczeń Cisco, dlatego najlepiej będzie współpracować z pozostałymi produktami tego samego dostawcy.

To chyba największa zaleta ISE, że daje możliwość integracji z rozwiązaniami i urządzeniami innych producentów, np. firewall'ami czy rozwiązaniami MDM. Na podstawie reguł pochodzących z zewnętrznego systemu możemy zarządzać dostępem do sieci. Jeśli coś się stanie np. z urządzeniem mobilnym i nie będzie ono zgodne z polityką, np. ze względu na nieaktualny system lub zostanie wykryty jakiś malware, to możemy połączyć to IP z konkretnym urządzeniem i takie urządzenie nie zostanie wpuszczone lub będzie wyizolowane.

– Krzysztof Osmałek, Senior Systems Engineer, Advanced Services Team Lead

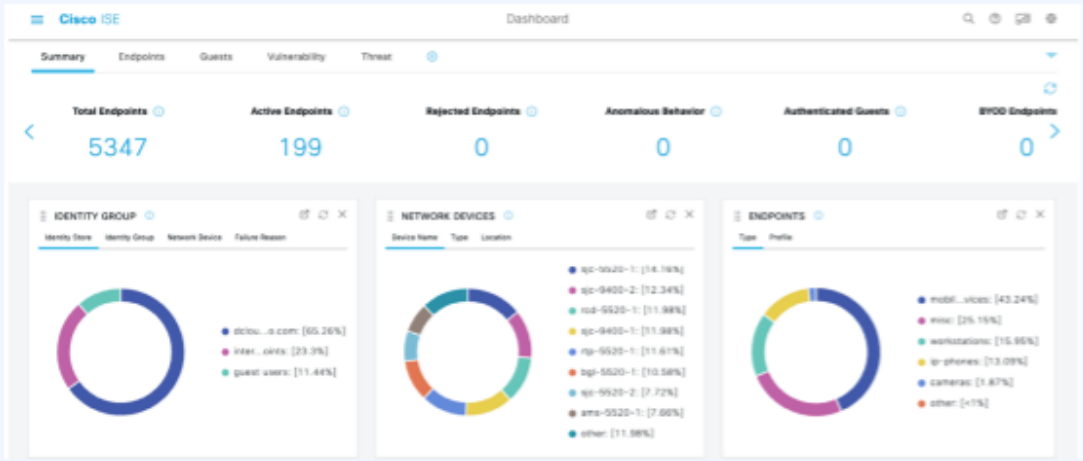
Wygoda

W ciągu ostatnich 10 lat cały czas ewoluował i dostosowywał do bieżących trendów. Dashboard jest przyjemny, intuicyjny i przede wszystkim łatwo układa się reguły związane z polityką.

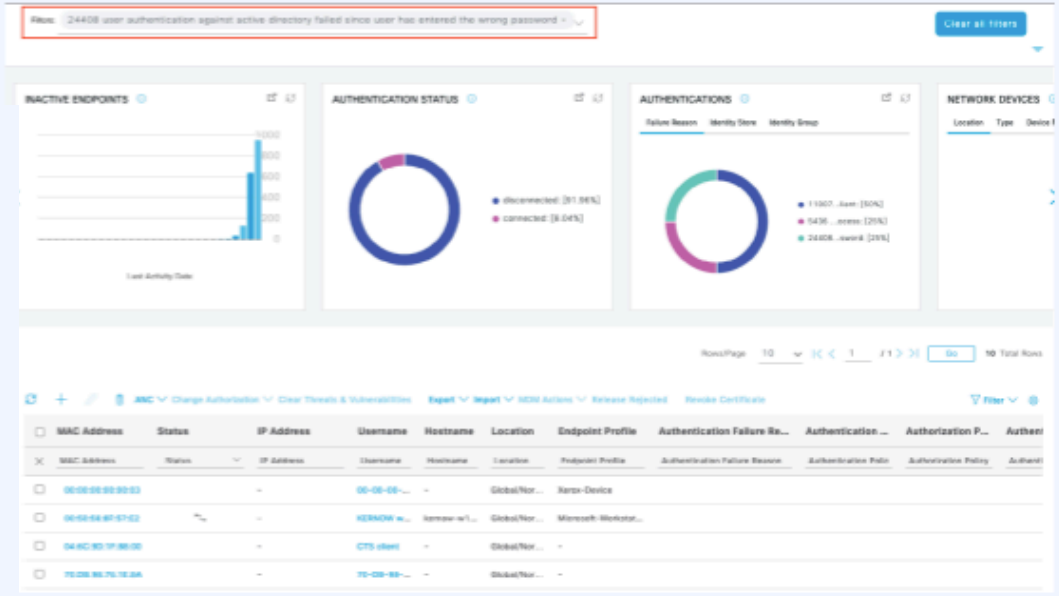
Cały wachlarz filtrów pozwala w ławy sposób przeglądać interesujące nas zdarzenia, a dedykowana wyszukiwarka doprowadzi nas prosto do celu.

Jest to szczególnie ważne przy dużych sieciach, gdzie tych logów są tysiące. Klikając na dany event, nie dostajemy tylko informacji o statusie, ale również całą konwersację urządzenia z siecią – również historycznie.

– Marcin Biały, Advisory Architect



Widoczność endpointów w panelu Cisco ISE

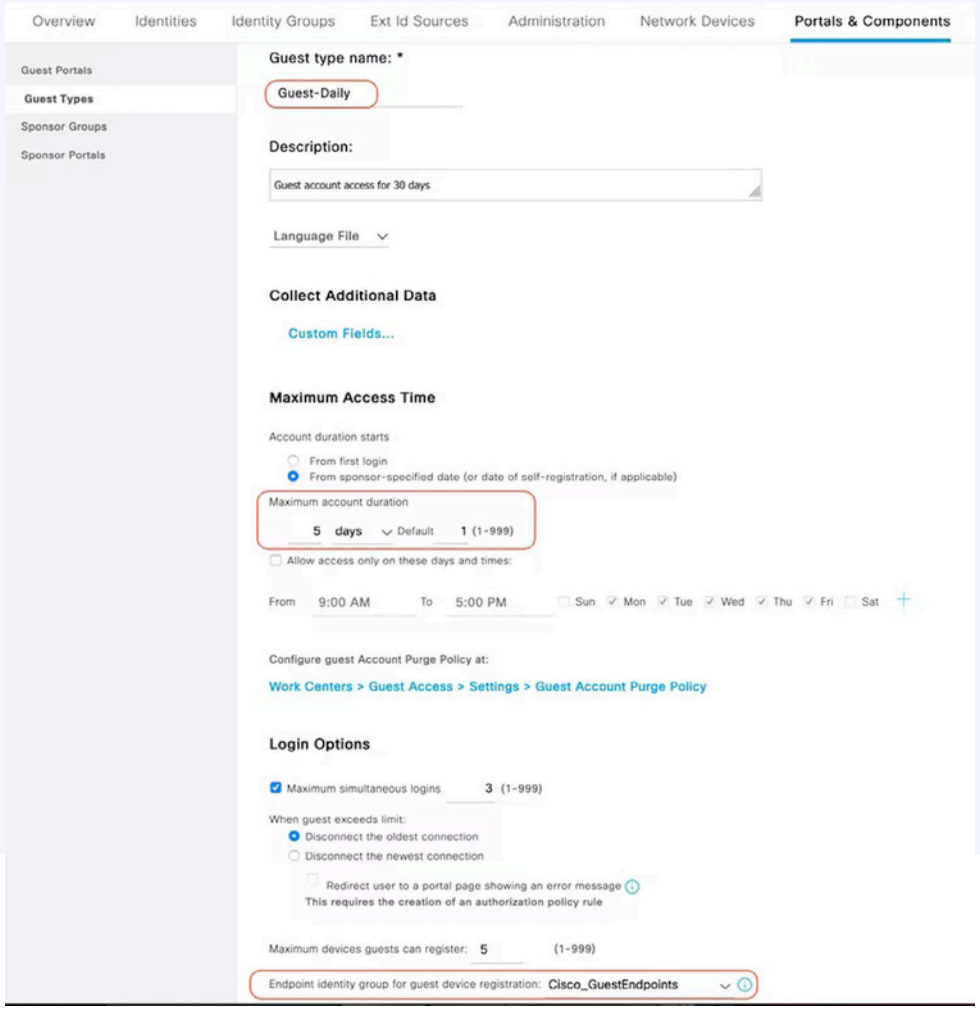


Zaawansowane filtrowanie zdarzeń w panelu Cisco ISE

Guest access

Guest Access to dostęp do sieci dla osób z zewnątrz, np. dla gości w hotelu. Nie tylko ogranicza dostęp do zasobów organizacji, ale na tym etapie NAC może ich odesłać do zupełnie innej sieci.

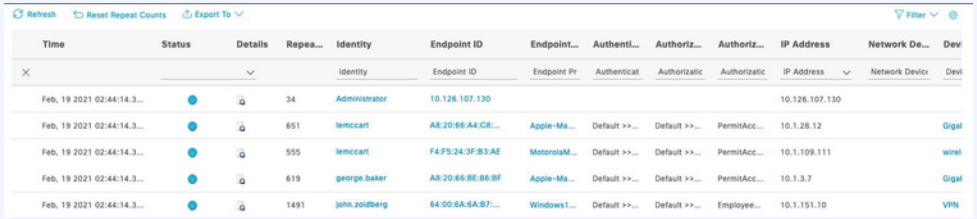
Cisco ISE posiada wiele różnych konfiguracji dostępu. Do najciekawszych należy self-onboarding, gdzie użytkownik sam definiuje dostęp do sieci, podając podstawowe dane, oraz sponsoring – wygenerowanie hasła przez osobę wewnątrz organizacji, która bierze niejako odpowiedzialność za swoich gości. Na uwagę zasługuje także dopracowany mechanizm BYOD (bring your own device) pozwalający na podłączenie prywatnych urządzeń użytkowników danej organizacji, ale z zachowaniem uwierzytelnienia 802.1x za pomocą certyfikatów generowanych “w locie”.



Konfiguracja dostępu gościnnego w Cisco ISE

Raportowanie

Wygoda przeglądania zdarzeń logowania i aktywnych sesji dostarczających danych o urządzeniach podłączonych jest najważniejszą cechą Cisco ISE. Granularny zestaw parametrów danej sesji AAA to zaleta dla każdego administratora. Istnieje rów- nież możliwość raportowania, jednak wykorzystywana jest ona najczęściej jedy- nie jako dokument potrzebny podczas kontaktu z supportem. Pod tym względem Cisco ISE się nie wyróżnia.



Dane o zalogowanych urządzeniach w Cisco ISE

Support

Jeśli nie znajdziemy odpowiedzi na jednym z oficjalnych, moderowanych przez inżynierów i prężnie działających forów, zakładane jest zgłoszenie w dedykowanym systemie wsparcia. Konsultant, który zostaje przypisany do sprawy, specjalizuje się w obszarze naszego problemu. Prowadzi cały proces i w razie potrzeby dokonuje interwencji.

Dodatkowe zalety

Poza opisanymi we wcześniejszej części możliwościami integracji i profilingiem, Cisco w wyższych modelach licencyjnych posiada również funkcję posturę assesment. Już po uwierzytelnieniu, ale jeszcze przed połączeniem, NAC wysyła do suplikanta, fragmentu oprogramowania na urządzeniu, prośbę o informację o zabezpieczeniach, systemie i parametrach, które mogą wpłynąć na bezpieczeństwo sieci.

Licencja na Cisco ISE

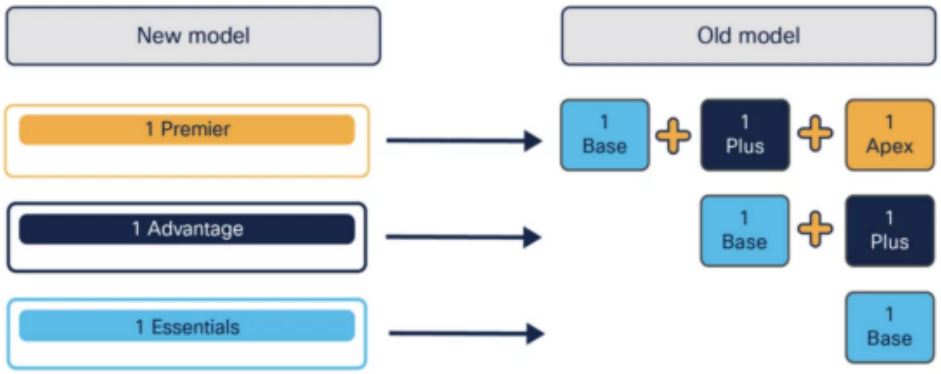
Ci, którzy znają i używają Cisco ISE, przyzwyczaili się do systemu licencjonowania znanego z ISE 1.x i 2.x. Dobrze znane licencje Base, Plus i Apex kończą swój żywot wraz z pojawieniem się ISE 3.X. W ich miejsce pojawiły się licencje tzw. Tier Based, czyli Essentials, Advantage i Premier.

Licencje Base były dotychczas licencjami permanentnymi, czyli raz kupione, nie wygasały. Inaczej było z Plus i Apex. Od ISE 3.0 wszystkie licencje są czasowe! (Tier-based licenses). Jakie funkcjonalności znajdziemy w poszczególnych poziomach licencyjnych? To jest bardzo dobrze opisane między innymi w Licensing Guide.

Kolejną różnicą jest podejście do funkcjonalności oraz „składania" licencji dla naszych potrzeb. Mimo, że mniej więcej nowe licencje można traktować analogicznie pod kątem funkcjonalności, które zapewniają, czyli:

- Base – Essentials
- Plus – Advantage
- Apex – Premier

W ISE 3.0 licencje wyższe zawierają w sobie licencje niższe (tzw. Nested doll model). Oznacza to, że wystarczy kupić licencję Advantage, żeby mieć funkcjonalność licencji Essentials + Advantage. W starym modelu dodawało się różne poziomy licencyjne, były też wymagania posiadania minimalnej liczby licencji Base do posiadania X licencji wyższych i tak dalej.



Jak liczymy licencje ISE?

Ceny licencji Cisco ISE są uzależnione od wielkości pakietu, czyli liczby licencji które kupujemy. W skrócie 10 000 licencji będzie tańsze niż 2000 licencji w przeliczeniu na 1 licencję.
Licencje liczymy per urządzenie, a nie użytkownika! Pamiętać należy o tym, że jeden użytkownik zalogowany i uwierzytelniony do sieci mechanizmem 802.1x wired + w tym samym czasie 802.1x wireless będzie konsumował 2 licencje! Licencjonowanie opiera się na liczbie jednocześnie połączonych urządzeń / enpoint'ów / adresów MAC do sieci.

ISE Virtual Appliance

Uwaga! Od ISE 3.1, Cisco waliduje licencje na tzw. Node VM. Jeśli nasz deployment (instalacja ISE) jest złożony np. z 5 węzłów, tzw node'ów, należy kupić 5 licencji w zależności od tego, jak duża maszyna wirtualna jest potrzebna. Jeśli tego nie zrobimy, ISE będzie upominać się o taką licencję (per node) i wyśle stosowne ostrzeżenia.

Cena licencji w tym przypadku zależy od wielkości VM appliance, a to z kolei od dobranego do skali rozwiązania obrazu VM. Tutaj mamy następujące możliwości:

- VM Small
- VM Medium
- VM Large

Którą kiedy wybrać? O tym mówi guideline producenta. Ale jeśli nie lubisz takiej lektury – **daj znać**, możemy wspólnie to przeanalizować dla Twojego środowiska.

Podsumowanie

Ponad wszelką wątpliwość należy mieć system NAC w swojej infrastrukturze. To, jaki system wybrać zależy w dużej części od możliwości finansowych danej organizacji i środowiska, w jakim funkcjonuje. Systemy NAC powodują, że administracja dostępami do sieci sprowadza się do budowy spójnej polityki i reguł NAC, w fazie operacyjnej, NAC kontroluje samodzielnie i dynamicznie połączenia do sieci w skali całej firmy dynamicznie przyznając (bądź nie) dostęp do infrastruktury, a także autoryzując poszczególnych użytkownikow i urządzenia. NAC jest nieoce- niony w przypadku dużych sieci, gdzie w znacznym stopniu ułatwia indeksowanie, ustawianie dostępów i zarządzanie użytkownikami. W mniejszych firmach ma wiele plusów, jednak warto zastanowić się nad równowagą pomiędzy kosztami a przydatnością całego systemu.

Co jeszcze warto rozważyć przed inwestycją w NAC?

- Jak często osoby spoza organizacji podłączają się do sieci?
- Jakie są fizyczne zabezpieczenia sieci?

W pewnej skali nie da się tego przypilnować ręcznie i z niepoukładaną infrastrukturą. Można próbować skryptów, pisać swoje rozwiązania, programować wokół sieci, jednak w pewnym momencie dojdziemy do momentu, gdzie to, co napisaliśmy, staje się NACiem.

– Marcin Biały, Advisory Architect

OGÓLNE WRAŻENIA I ZASTOSOWANIE	
polska wersja językowa panelu	
polski support	
anglojęzyczny support	✓
angielska wersja językowa panelu	✓
dla każdego typu organizacji	✓
dobrze rozpoznawalne rozwiązanie	✓
część większego ekosystemu producenta	✓
licencjonowana pełna funkcjonalność	
licencjonowane poszczególne moduły / funkcjonalności	✓
dostępna wersja darmowa	
WDROŻENIE I KONFIGURACJA	
duży wachlarz dodatkowych funkcjonalności	✓
duże możliwości automatyzacji	
duże możliwości ustalania reguł	✓
duże możliwości filtrowania	✓
profiling	✓
wsparcie dla CoA	✓
duża widoczność urządzeń	✓
obsługa TACACS+	✓
podgląd na żywo (autoryzacja sesji)	✓

NIEZAWODNOŚĆ	
redundancja	✓
wirtualne maszyny	✓
wysoce skalowalne	✓
regularne aktualizacje	✓
WYGODA UŻYTKOWANIA	
intuicyjny interfejs	✓
łatwo dostępne informacje o logach	✓
nowoczesny interfejs	✓
łatwy we wdrożeniu	✓
pracochłonna konfiguracja przy większej złożoności wymagań	✓
wysoka stabilność systemu	✓
obszerna dokumentacja	✓
GUEST ACCESS	
dostępny przy zakupie bazowego produktu	✓
duże możliwości personalizacji	✓
prostota wykorzystania	✓
self onboarding	✓
sponsoring	✓
BYOD	✓

INTEGRACJE	
integracja z API systemów zewnętrznych	✓
gotowe moduły integracji	
integracja MDM	✓
RAPORTOWANIE	
dostępne w podstawowej wersji systemu	✓
raportowanie do pdf	✓
możliwość wyeksportowania danych	✓
dostępne moduły analityczne	
atrakcyjnie wizualne raporty	✓
SUPPORT	
aktywne community	✓
support producenta	✓
sprawny support	✓
sformalizowane podejście supportu	✓
dedykowany opiekun klienta	

DODATKOWE ZALETY	
aplikacja do konfiguracji urządzeń końcowych	
bezkosztowe rozszerzenie środowiska po zakupie licencji	✓
Posture Assessment	✓
obsługa eduroam	✓
możliwość mikrosegmentacji	✓
wykorzystuje Sztuczną Inteligencję	

Materiały dodatkowe

Dobre praktyki

Buduj na solidnych fundamentach

Jeśli nie wiesz, jak zbudować politykę dostępu do sieci – zbuduj tak, aby system NAC był jej integralnym komponentem. W pierwszym etapie możesz uruchomić system jedynie w trybie monitoringu. Poznasz urządzenia mające dostęp do sieci, zachowania użytkowników i dopiero na podstawie własnych obserwacji przejdziesz do stworzenia reguł, które będą skuteczne i specyficzne dla Twojej organizacji.

Wdrażaj po kolei

I przykładaj dużą wagę do testów. W praktyce najpierw zainstaluj system, następnie konfiguruj urządzenia sieciowe (NAD), a dopiero w kolejnym kroku, rób tzw. rollout lokalizacja po lokalizacji, dając szansę na mimi-nalny wpływ na działanie biznesu w przypadku błędu.

Zapewnij redundancję

Buduj system na przynajmniej dwóch węzłach (instancjach), które będą w stanie obsługiwać zapytania. W ten sposób minimalizujesz ryzyko awarii, ponieważ w razie problemów, drugie urządzenie przejmie aktywnie rolę. Dla dużych sieci powinno być ich nawet więcej!

Działaj systemowo

Sprawdź, jakie urządzenia mają dostęp do sieci. Jeśli ujednolicisz ich zabezpieczenia, oszczędzisz sobie w przyszłości sporo pracy.

Konfiguracje

Modele deploymentu Cisco ISE

Jak dodać NAD do ISE 3.0

Jak dodać Cisco ISE do Active Directory

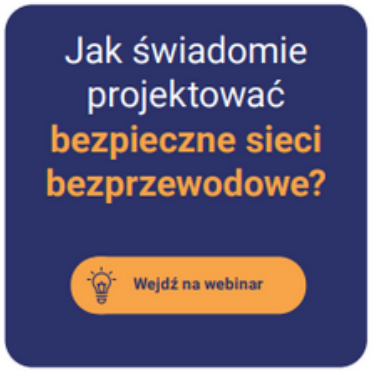
Blog posty

Jak projektować bezpieczne sieci Wi-Fi?

Jak działa system kontroli Cisco ISE?

Jak przetestować Cisco ISE za darmo?

Webinar



Autorzy

Marcin Biały, Advisory Architect

Przez ponad 15 lat pracował nad bezpieczeństwem sieci dla największych świa- towych dostawców sieci jako Network Architect, Leading Architect czy Technical Solution Manager, przygotowując i realizując projekty oraz odpowiadając za mi- gracje infrastruktury. Posiada takie certyfikaty jak CCNP, CCNA, CCSI #35269, FCNSP #7207, FCNSA i wiele innych.

Krzysztof Osmałek, Senior Systems Engineer, Advanced Services Team Lead

Sieciami zajmuje się od ponad 16 lat, przez niemal całą swoją karierę w IT. Karierę rozpoczynał od administrowania siecią, a następnie zajmował się m.in. bezpie- czeństwem czy koordynowaniem projektów sieciowych. Z Grandmetric jako in- żynier sieciowy i leader zespołu Advanced Services związany jest od 2019 roku. Odpowiada za wdrożenie, przygotowanie i koordynację projektów. Certyfikowany inżynier Cisco i innych vendorów, CCNP, CCDP czy GM Ware.

Grandmetric

To istniejący na rynku od 2015 roku polski integrator systemów IT o międzynarodowym zasięgu, skupiający się na rozwiązaniach sieciowych – zarówno tych bezprzewodowych jak i tradycyjnych. Eksperci Grandmetric łączą pasję do technologii i lata doświadczenia w zawodzie projektując, a następnie wdrażając kompleksowe rozwiązania informatyczne, wspierając migrację danych i monitorując infrastrukturę klientów. Umiejętności ekspertów potwierdzone są licznymi case studies oraz certyfikatami największych dostawców takich jak Microsoft, AWS, Cisco, Palo Alto i wielu innych.

Wybierz dla siebie NACa

Potrzebujesz wsparcia w zrozumieniu systemu NAC lub zabezpieczeniu swojej sieci?

Pomożemy Ci skonfigurować Twoje zabezpieczenia

W ramach konsultacji pomożemy Ci dobrać odpowiednie systemy security i nauczymy Cię je konfigurować i monitorować.

- identyfikujemy luki w bezpieczeństwie organizacji
- układamy procedury bezpieczeństwa
- projektujemy bezpieczne sieci i systemy
- dostarczamy i konfigurujemy rozwiązania bezpieczeństwa na każdym poziomie organizacji
- szkolimy z wdrażanych rozwiązań

Porozmawiajmy

sales@grandmetric.com

+48 612 710 443

Przygotujemy PoC

Proof of Concept (PoC) to usługa, w ramach której doświadczony inżynier przygotowuje instalację wybranego systemu w Twojej organizacji. Dzięki temu możesz w praktyce zobaczyć, jak poradzi sobie dane rozwiązanie w rzeczywistych warunkach.

Po zakończeniu PoC, decydujesz, czy instalujesz rozwiązanie na stałe, czy rezygnujesz.

- ograniczasz ryzyko
- testujesz rozwiązanie w praktyce
- masz wsparcie inżyniera Grandmetric

Porozmawiajmy

sales@grandmetric.com

+48 612 710 443