NARODOWY INSTYTUT ZDROWIA PUBLICZNEGO
PAŃSTWOWY INSTYTUT BADAWCZY

niepodległa

OPIS PRZEDMIOTU ZAMÓWIENIA

Wdrożenie rozwiązania do zarządzania oraz kontrolowania sieci LAN klasy NAC wraz z dostawą rocznej subskrypcji na licencje

W ramach postępowania należy dostarczyć licencje na redundantny serwer uwierzytelniania oraz współpracę z 22 przełącznikami HP ProCurve 28x posiadanymi przez Zamawiającego.

Minimalne wymagania dla systemu kontroli dostępu do sieci LAN klasy NAC

I. Architektura

1. Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci.
   a. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux lub jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare
   b. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS
2. Wszystkie elementy Sytemu powinny być zarządzane centralnie.

II. Funkcje systemu

1. Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli
2. Aplikacja zarządzająca musi zarządzać wszystkimi oferowanymi urządzeniami oraz wszystkimi dostarczonymi punktami dostępowymi.
3. Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników

4. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
5. Aplikacja zarządzająca musi pozwalać na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
6. Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
7. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
8. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
9. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
10. Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych.
11. Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu.
12. Aplikacja musi posiadać wbudowany Syslog serwer.
13. Aplikacja musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps
14. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
15. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
16. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
17. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem

a. połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu
b. konfiguracji sieci VLAN

18. Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https

19. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
    a. adres IP urządzenia
    b. adresu MAC urządzenia
    c. nazwy urządzenia
    d. wersji oprogramowania
    e. wersji bootrom
    f. lokalizacji urządzenia
    g. danych kontaktowych administratora
    h. numeru seryjnego
    i. numeru inwentaryzacyjnego – własna numeracja

20. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
    a. możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie
    b. możliwość realizacji backup'u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych
    c. możliwość odtworzenia wskazanej konfiguracji urządzenia
    d. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami
    e. możliwość obsługi backup'u urządzeń sieciowych różnych producentów

21. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie

22. Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
23. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
24. Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd, CCTV, Access Point itp.
25. Aplikacja musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem:
    a. przyłączenia do sieci VLAN
    b. przyłączenia do serwisu w ramach „Fabric" z wykorzystaniem IEEE 802.1Qcj,
    c. konfiguracji Quality of Service
    d. konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4
    e. możliwości wyłączenia uwierzytelniania wielu użytkowników na porcie – np. w przypadku polityki Access Point, gdzie uwierzytelnienie użytkowników jest przeniesione z portu przełącznika do punktu dostępowego lub kontrolera sieci bezprzewodowej.
26. Aplikacja zarządzająca musi zapewniać zarządzanie siecią bezprzewodową.
    a. Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
    b. Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac, IEEE 802.11ax
    c. Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
        - adres IP kontrolera
        - liczba obsługiwanych klientów
        - szczytowe wartości zajmowanego pasma
        - wersja oprogramowania

d. Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
    - adres IP punktu dostępowego
    - MAC adres punktu dostępowego
    - wersja oprogramowania
    - typ punktu dostępowego
    - kanały pracy poszczególnych interfejsów radiowych
    - szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych

e. Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
    - adres IP klienta
    - MAC adres klienta
    - nazwa użytkownika
    - nazwa punktu dostępowego, do którego dołączony jest użytkownik
    - BSSID, do którego dołączony jest użytkownik
    - SSID, do którego dołączony jest użytkownik

f. Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
    - zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
    - zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem
    - lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych

27. Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji:
    a. adresu MAC
    b. adresu IP

c. nazwy komputera
d. typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / iOS itp.
e. nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
f. adres IP urządzenia, do którego dołączony jest klient.
g. identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
h. typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.
i. nazwa przydzielonej polityki bezpieczeństwa.

28. Przydział urządzenia do grupy urządzeń powinien być możliwy poprzez dodanie MAC adresu urządzenia do grupy oraz przez wskazanie uwierzytelnionego urządzenia na liście i przeniesienia go do wskazanej grupy – w celu uniknięcia konieczności przepisywania MAC adresów urządzeń.
29. System portalu www służący do rejestracji gości musi zapewniać obsługę gości w języku min. polskim, angielskim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa.
30. System zarządzania musi pozwalać na analizę ruchu w sieci do warstwy 7
31. Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji.
32. Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji.
33. System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos

34. System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji.
35. Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji.
36. System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacje we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp.
37. System Analityki musi zapewniać możliwość tworzenia raportów.
38. System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu na wskazany adres e-mail
39. System zarządzania musi posiadać możliwość tworzenia skryptów CLI i Python, które pozwolą na uproszczenie zarządzania siecią poprzez wykonywanie tych samych operacji na wielu urządzeniach lub zapewnią automatyzację poprzez ich uruchomienie na podstawie różnorodnych zdarzeń występujących w Aplikacji Zarządzającej, Systemie Analityki, Systemie zarządzania tożsamością.
40. System zarządzania musi posiadać możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora)
41. System zarządzania musi posiadać możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu. Alarm musi zapewniać przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie.
42. System zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub periodycznie (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czasu
43. System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki
44. System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów:

a. Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami firewall Fortinet posiadanymi przez Zamawiającego.
b. Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny
c. Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – Microsoft Intune, AirWatch MDM

45. Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
46. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
    a. szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
    b. wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
    c. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
    d. generowanie raportów

III. System zarządzania tożsamością

1. System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.

2. System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
3. System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie:
    a. Typu uwierzytelnienia – np. IEEE 802.1x PEAP, IEEE 802.1x TLS, IEEE 802.1x TTLS, MAC Authentication, logowanie do urządzenia za pomocą Telnet lub SSH, logowanie użytkownika poprzez Captive Portal itp.
    b. Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika.
    c. Realizacji przyłączania do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC
    d. Realizacji przyłączenia do sieci ze wskazanej „lokalizacji" – możliwość wyboru, czy dotyczy to sieci przewodowej, czy bezprzewodowej, adresu IP urządzenia, które zapewnia uwierzytelnianie, numeru portu lub ich zakres, SSID w przypadku sieci bezprzewodowej itp.
    e. Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia
4. System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List, grupa drukarek itp.
5. System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
6. System zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS

7. System zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. PESEL, nr. Dokumentu tożsamości, adres email, numer telefonu, adres email osoby zapraszającej itp.
8. System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy.
9. System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
    a. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
    b. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
    c. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, iOS, Android
    d. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
    e. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
10. System zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python – przykładowo musi zapewniać możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication
11. System zarządzania tożsamością zautoryzowanych klientów, jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę minimum 1 000 urządzeń klienckich (adresów MAC) przez okres minimum 1 roku.

IV. Alarmy

1. Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych.
2. Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia.

3. Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak:
    a. Wysłanie e-mail do wskazanej grupy adresowej
    b. Wysłanie informacji SYSLOG do wskazanego serwera
    c. Wysłanie TRAP SNMP do wskazanego adresu IP
    d. Uruchomienie skryptu w systemie operacyjnym Linux
    e. Uruchomienie skryptu skonfigurowanego w systemie zarządzającym

V. Wdrożenie

1. Wdrożenie musi być przeprowadzone w taki sposób, aby nie zakłócało bieżącej działalności Zamawiającego
2. Wykonawca musi wykonać usługę wdrożenia zaoferowanego systemu w postaci instalacji systemu, konfiguracji polityk dostępowych, integracji z posiadaną przez Zamawiającego infrastrukturą Fortinet w celu dwustronnej komunikacji. Wdrożenie musi przeprowadzić inżynier posiadający aktualny certyfikat techniczny oferowanego systemu oraz ważny certyfikat co najmniej NSE 4 - FortiGate Network Security Professional

VI. Szkolenie

1. Zamawiający wymaga przeszkolenia 5 pracowników Działu Informatycznego w zakresie dostarczonego i wdrożonego oprogramowania systemu kontroli dostępu do sieci LAN klasy NAC w formie online lub stacjonarnie w siedzibie u Zamawiającego
2. Szkolenie powinno trwać nie krócej niż 1 dzień roboczy, tj. 6 godzin i powinno obejmować co najmniej:

a) proces instalacji;
b) konfigurację systemu;
c) omówienie sposobu zarządzania systemem z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową;
d) konfigurację praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania;

e) tworzenie map graficznych umiejscowienia urządzeń sieciowych, końcowych, gniazdek internetowych z podziałem na budynki, pokoje oraz węzły sieciowe;
f) zarządzanie urządzeniami sieciowymi;
g) tworzenie i egzekwowanie zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej;
h) omówienie integracji z systemami zewnętrznymi
i) generowanie raportów oraz monitoring systemu;
j) generowanie alarmów systemowych

VII. Wsparcie

System zarządzania musi być objęty 12 miesięcznym wsparciem serwisowym producenta

Powyższe parametry określone w niniejszym Opisie Przedmiotu Zamówienia są parametrami minimalnymi.