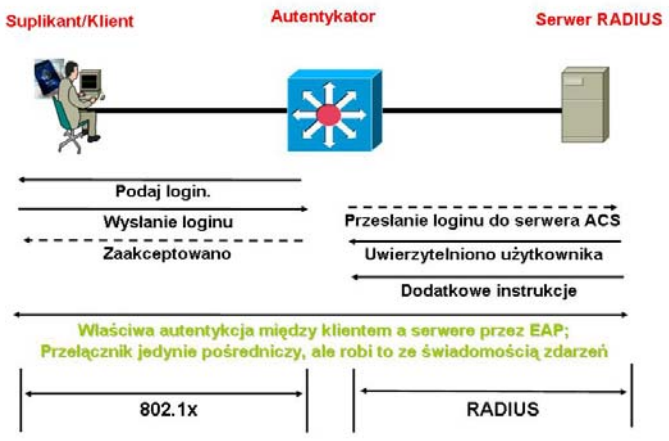
Jak żyć w zgodzie z instrukcją kancelaryjną ?

Standard 802.1x jako mechanizm uwierzytelniania w sieci Urzędu.

*Czas ostatnich miesięcy to w Jednostkach Samorządu Terytorialnego (**JST**) okres bardzo dynamicznego wdrażania usług związanych z e-Urzędem. Wprowadzenie nowych funkcji mających na celu usprawnienie obsługi obywatela napotyka jednak na wyzwania związane ze spełnieniem uregulowań związanych z zabezpieczeniem danych urzędu. Należy do nich m.in. **instrukcja kancelaryjna**, która nakazuje izolowanie środowisk wewnętrznych urzędów od środowisk przyłączonych do globalnej sieci internet.*

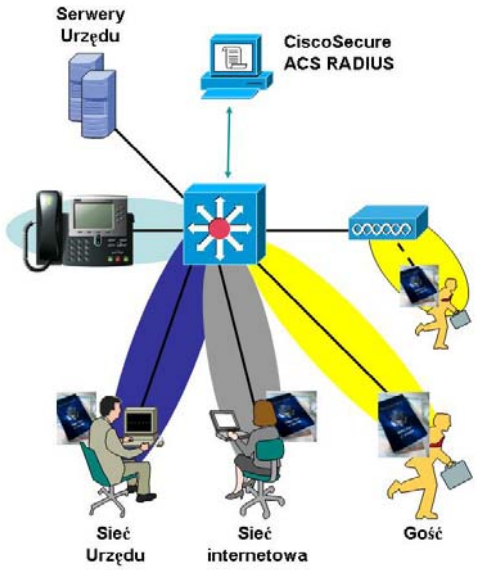
Spełnienie wszystkich wymagań instrukcji kancelaryjnej dotyczących przyłaczenia urzędu do internetu jest trudne – chociażby z tego względu, że galwaniczna izolacja obu sieci stoi w sprzeczności z nowo budowanymi usługami, gdzie obywatel powinien mieć możliwość samodzielnego sprawdzenia statusu sprawy w urzędzie przez internet. Również inne regulacje prawne niejako negują wymóg fizycznej separacji sieci internetowej od sieci wewnętrznej. Wydaje się zatem naturalnym wyborem poszukiwanie sposobów logicznej separacji obu sieci na poziomie urządzeń aktywnych pracujących w urzędach. Jedną z takich opcji jest wdrożenie standardu IEEE 802.1x jako mechanizmu uwierzytelnienia do sieci.

Standard IEEE 802.1x określa mechanizmy pozwalające kontrolować dostęp użytkownika do sieci. Zakłada on, że pierwotnym ustawieniem portów przełącznika jest ich zablokowanie. Otwarcie portu odbywa się dopiero wówczas gdy użytkownik dokona logowania (uwierzytelnienia). Dla tego celu można wykorzystać takie elementy jak certyfikaty cyfrowe, hasła jednorazowe, można też skorzystać ze standardowych parametrów użytkownik/hasło.



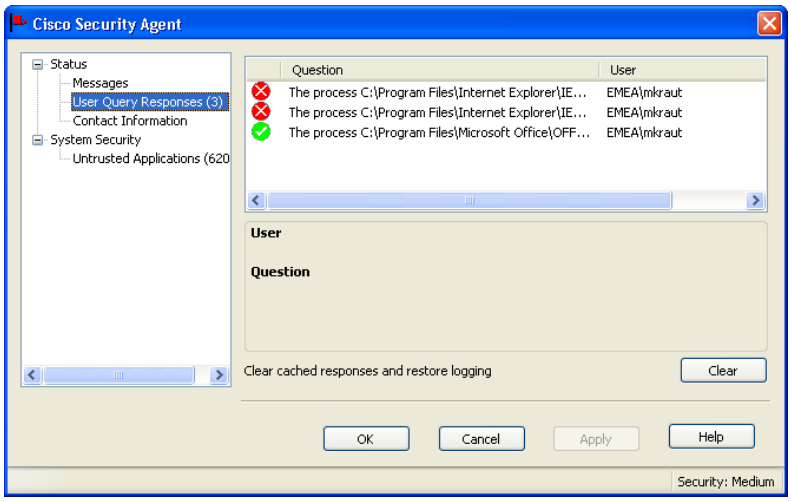
Na bazie przeprowadzonego uwierzytelnienia serwer sprawdzający tożsamość użytkownika może przesłać do przełącznika sieciowego dodatkowe parametry takie jak numer/nazwa sieci VLAN do którego powinien zostać przypisany port dany przełącznika, parametry związane z zapewnieniem jakości usług czy też przesłać profil bezpieczeństwa dla danego użytkownika.

Możliwy jest zatem scenariusz przestawiony poniżej: użytkownicy korzystają z jednego urządzenia – przełącznika sieciowego. Część użytkowników korzysta z zasobów wewnętrznych urzędu, inna część korzysta z zasobów internetowych. Przedstawiony scenariusz nie jest w żaden sposób ograniczony do kilku sieci VLAN. Oznacza to, iż przedstawiony mechanizm może być z powodzeniem wykorzystany do segmentacji sieci w większych jednostkach administracji samorządowej.



Bardzo ważnym elementem jest jednoznaczne zróżnicowanie dostępu użytkowników na poziomie logowania. Użytkownik logujący się do sieci jako Jan.Kowalski będzie przypisany do sieci VLAN o nazwie URZAD i będzie mógł korzystać z zasobów wewnętrznych. Ten sam użytkownik aby skorzystać z zasobów internetowych będzie musiał zalogować się na inne konto Jan.Kowalski.INET. Wprowadza to element świadomego korzystania z internetu przez użytkownika (konieczność logowania) oraz element jednoznacznej identyfikacji użytkownika przez administratora.

W przypadku **bardzo częstego modelu działania**, w którym jedna stacja robocza służy zarówno do korzystania z informacji wewnętrznych jak i tych dostępnych w sieci internet, zaleca się wprowadzenie dodatkowego systemu zabezpieczenia samej stacji przed atakiem (aplikacje antywirusowe oraz aplikacje wykrywania włamań i nadużyć na hostach – Host IPS).



Rozwiązania Cisco Systems umożliwiają dodatkowo kontrolę działania tychże przed dopuszczeniem użytkownika do danego segmentu sieci. Oznacza to że użytkownik, który chce korzystać z sieci internetowej poza oczywistą koniecznością zalogowania się do sieci będzie musiał uprzednio sprawdzić czy włączony jest klient systemu antywirusowego oraz agent Host IPS (HIPS). W przypadku gdy dana stacja ma wyłączone systemy obronne nie zostanie dopuszczona do segmentu internetowego. Funkcjonalność ta stanowi część bardziej rozbudowanego systemu określanego jako Network Admission Contol (NAC).

Co zatem jest konieczne aby zbudować opisany system ? Lista obejmuje szereg opisanych już powyżej elementów.

- przełącznik sieciowy, który obsługuje funkcjonalność 802.1x wraz z możliwością przypisania VLAN oraz innych parametrów. Wymóg ten spełniają praktycznie wszystkie obecnie dostępne przełączniki Cisco.
- Serwer uwierzytelnienia i autoryzacji np. Cisco Secure Access Control System (może współpracować z zewnętrzną bazą danych użytkowników np. z MS AD, bazami dostępnymi przez LDAP etc.)
- System Host IPS, np. Cisco Security Agent wraz z konsolą zarządzającą
- Systemy antywirusowe

Przedstawiony system pozwala zatem na zbudowanie bezpiecznego mechanizmu korzystania z zasobów internetowych w urzędach. Nie tylko pozwala na logiczną izolację wewnętrznych zasobów sieciowych od sieci internetowej, ale gwarantuje scentralizowaną kontrolę dostępu

do obu z nich jak i pozwala na wymuszenie u użytkowników konkretnych mechanizmów zabezpieczeń przy żądaniu dostępu do sieci internetowe. Całość procesu jest zautomatyzowana oraz udokumentowana w logach zbieranych przez serwer uwierzytelnienia.

Zaproponowane rozwiązanie spełnia nowe wymagania dotyczące budowy e-Urzędu, spełnia także szereg wymogów precyzowanych przez instrukcję kancelaryjną. Ostateczną decyzję, dotyczącą możliwości zastosowania tego rozwiązania pozostawiamy Państwu, jako administratorom i użytkownikom systemów administracji samorządowej.

W razie dodatkowych pytań prosimy o kontakt z zespołem odpowiedzialnym za współpracę z **JST**:

govpl@external.cisco.com , +48 22 572 27 15

Wsparcie Handlowe:

Piotr Skirski	pskirski@cisco.com	+48 22 5722729
Beata Haber	wbeata@cisco.com	+48 22 5722715

Wsparcie Techniczne:

Michał Kraut	mkraut@cisco.com	+48 22 5722733

Więcej informacji o opisanych rozwiązaniach znajduje się na stronach internetowych Cisco Systems:

Przełączniki Cisco Catalyst

http://www.cisco.com/en/US/products/hw/switches/

802.1x

http://www.cisco.com/en/US/products/ps6662/products_ios_protocol_option_home.html

Oprogramowanie Cisco Secure Access Control Server

http://www.cisco.com/en/US/products/sw/secursw/ps2086/

Oprogramowanie Cisco Security Agent

http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html

Network Admission Control

http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html