Architektura Cisco TrustSec

Adam Obszyński

Systems Engineer, CCIE #8557

aobszyns@cisco.com

Agenda

1. Cisco TrustSec - co to jest?
2. Autoryzacja i wdrażanie polityk w sieci
3. Security Group Access
4. Integralność i poufność danych
5. NAC Appliance
   - Uwierzytelnianie
   - Sprawdzanie stanu maszyny
6. Podsumowanie

Tożsamość – dlaczego to takie ważne?

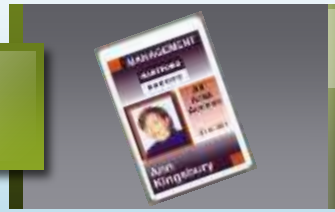
1

Kim jesteś?

802.1x (lub inna metoda) uwierzytelnia użytkownika

Trzymamy „obcych” z daleka

2



Dokąd masz dostęp?

Na podstawie uwierzytelnienia użytkownik trafia do odp. VLAN

Uczciwie traktujemy „naszych”

3

Jaki poziom usług otrzymujesz?

Użytkownik może otrzymać dostęp do usług indywidualnych (np. dACL)

Personalizujemy

4

Co robisz?

Tożsamość i lokalizacja mogą być użyte do śledzenia i rozliczania

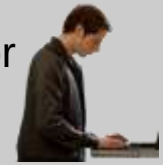
Podnosimy przejrzystość sieci

Wygodne i dopasowane reguły

Dopasowanie do biznesu

Tożsamość

Tożsamość:
Administrator sieci



Tożsamość:
Pracownik

Tożsamość:
Gość

Kasia Nowak
Pracownik
Kadry

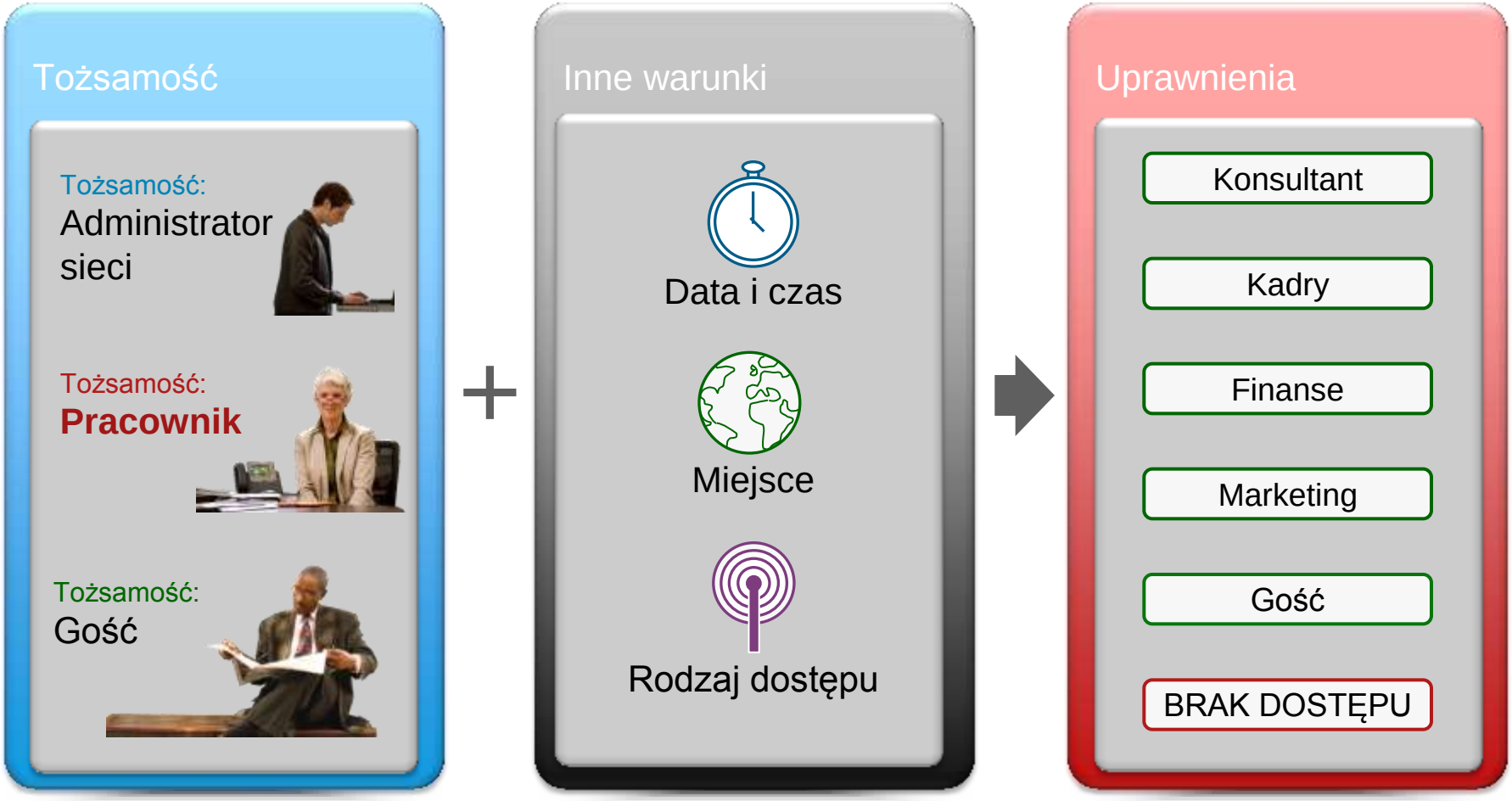
Każdy z nas pełni inną rolę

Zuzanna Kowalska
Pracownik
Dyrektor Sprzedaży

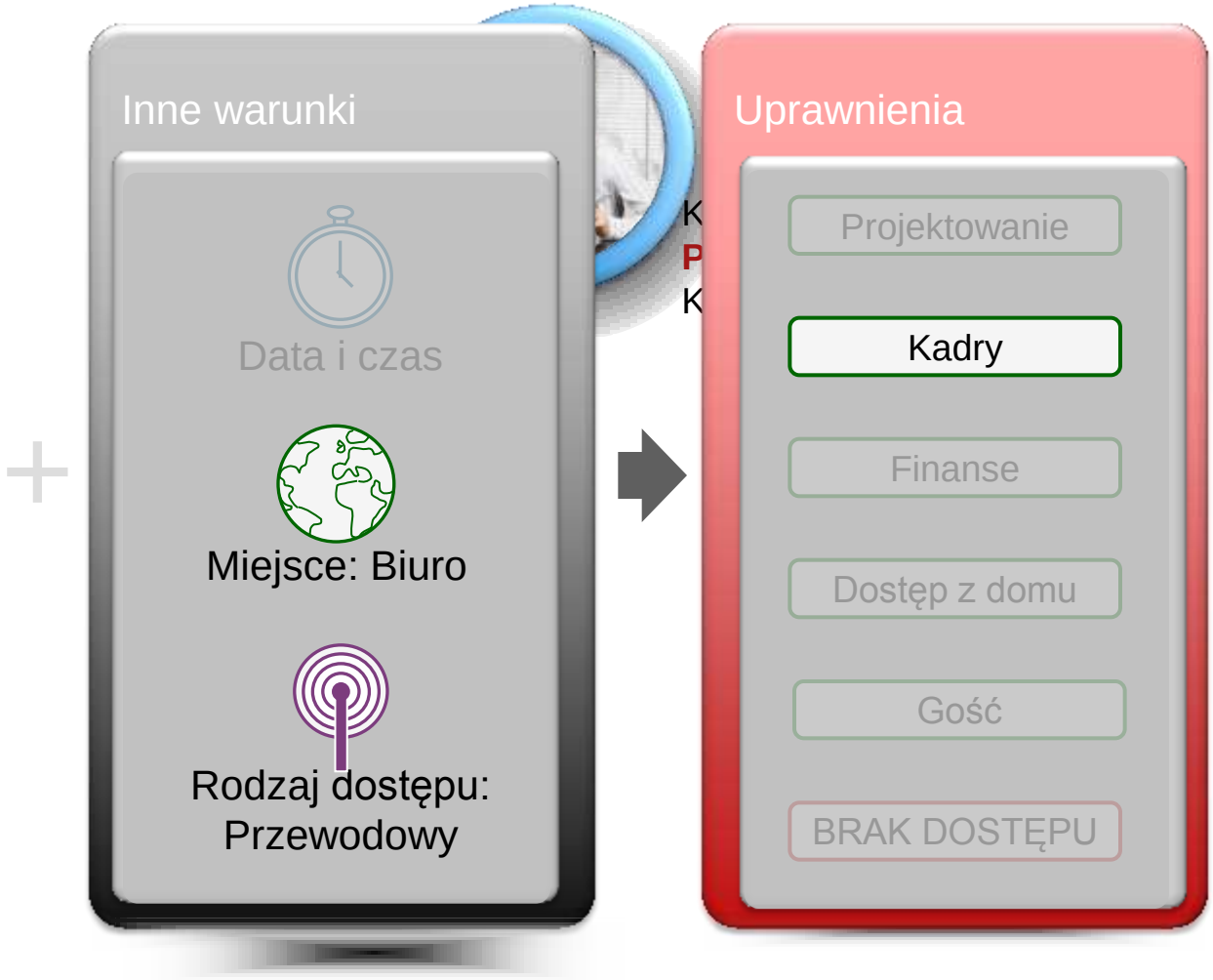
Franciszek Wiedza
Pracownik
Konsultant

Wioletta Syzyf
Pracownik
Marketing

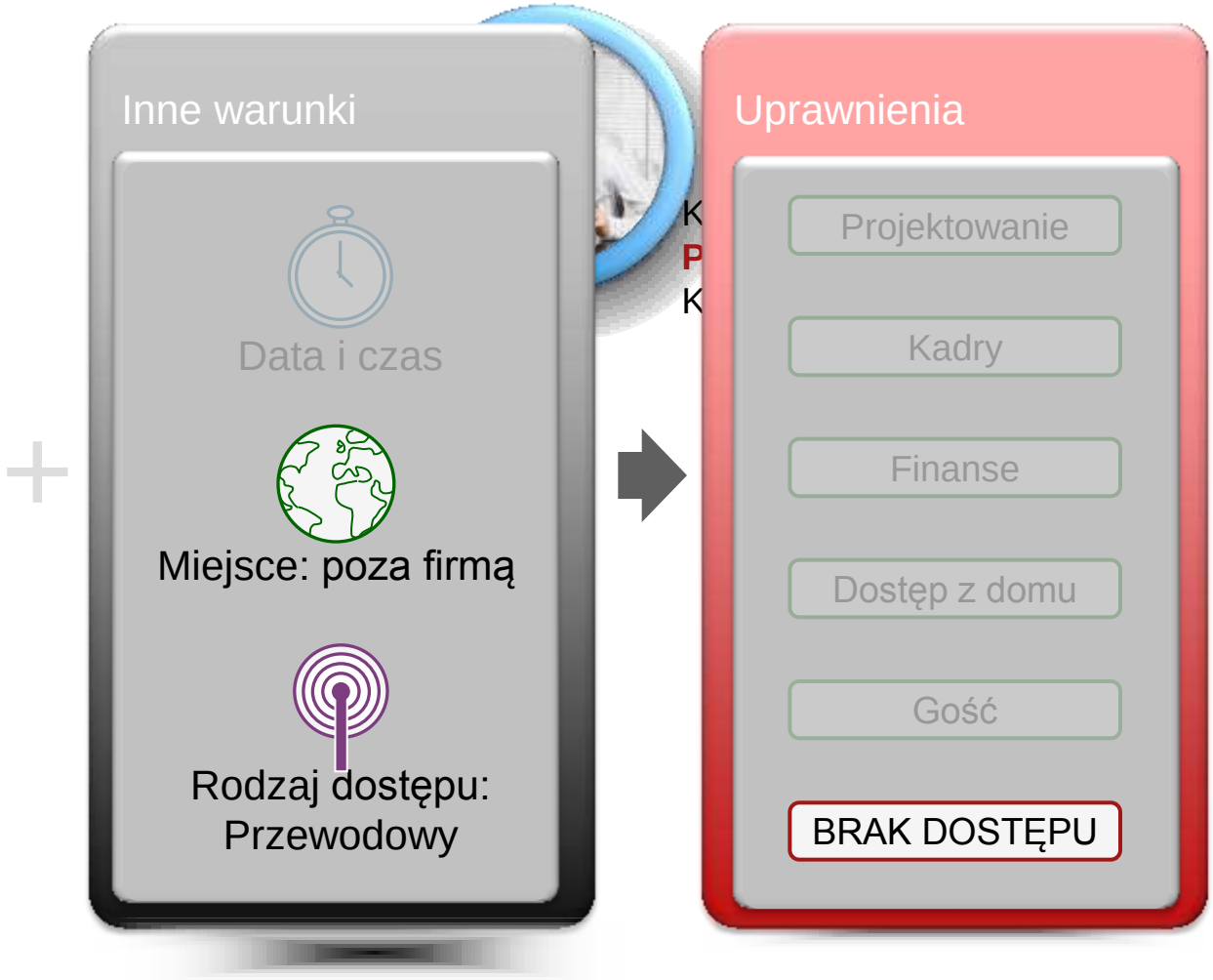
Reguły dzisiejszych wymagań biznesowych



Kontrola w modelu: rola + warunki
Przykład: Kadry



Kontrola w modelu: rola + warunki
Przykład: Kadry



Cisco TrustSec

Cisco TrustSec™

Pomaga klientom **zabezpieczać** swoje sieci, dane i zasoby poprzez:

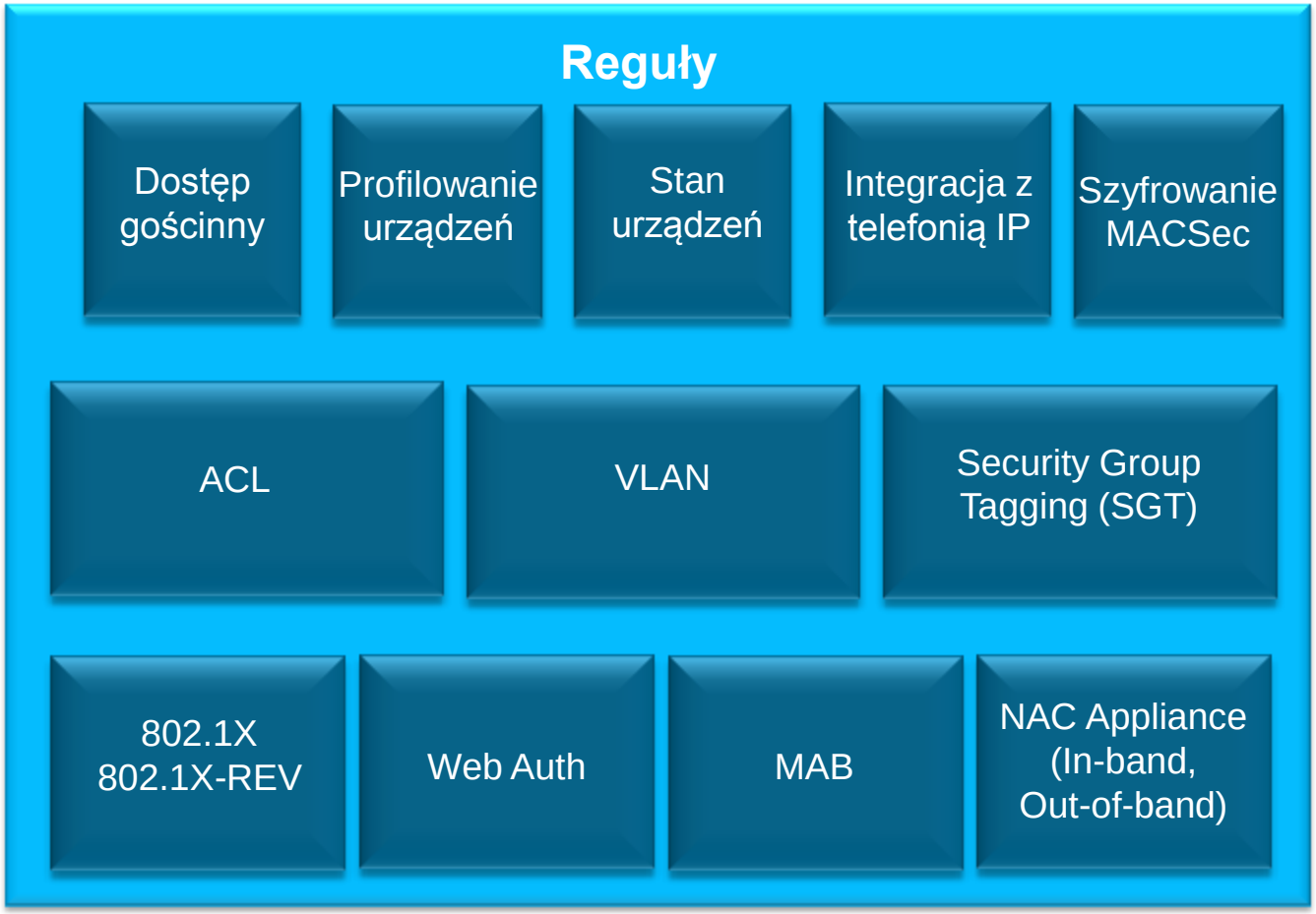
- Znajomość tożsamości użytkowników
- Opartą na regułach kontrolę dostępu
- Zapewnienie integralności i poufności danych

Architektura Cisco TrustSec™

Usługi dodatkowe

Autoryzacja

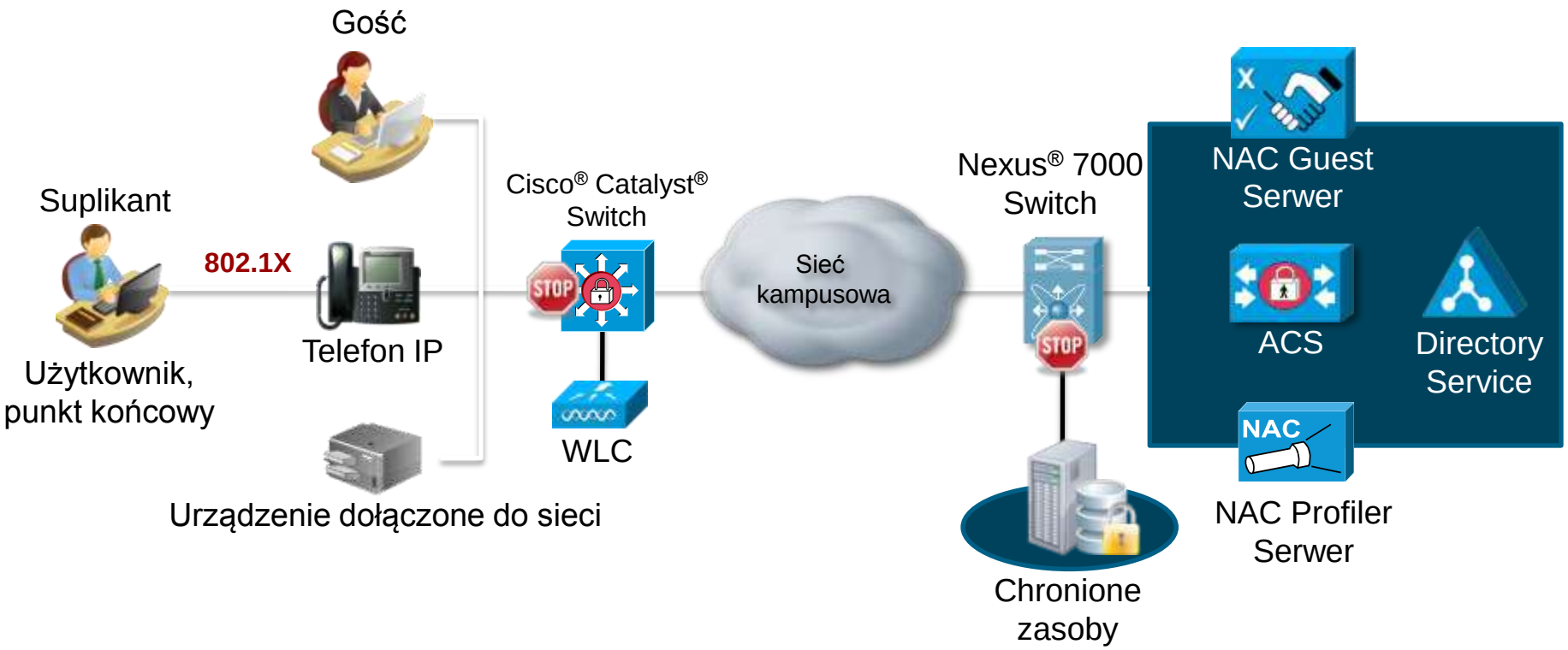
Uwierzytelnianie



MAB – MAC Authentication Bypass

Cisco TrustSec™

Kontrola dostępu w oparciu o 802.1X

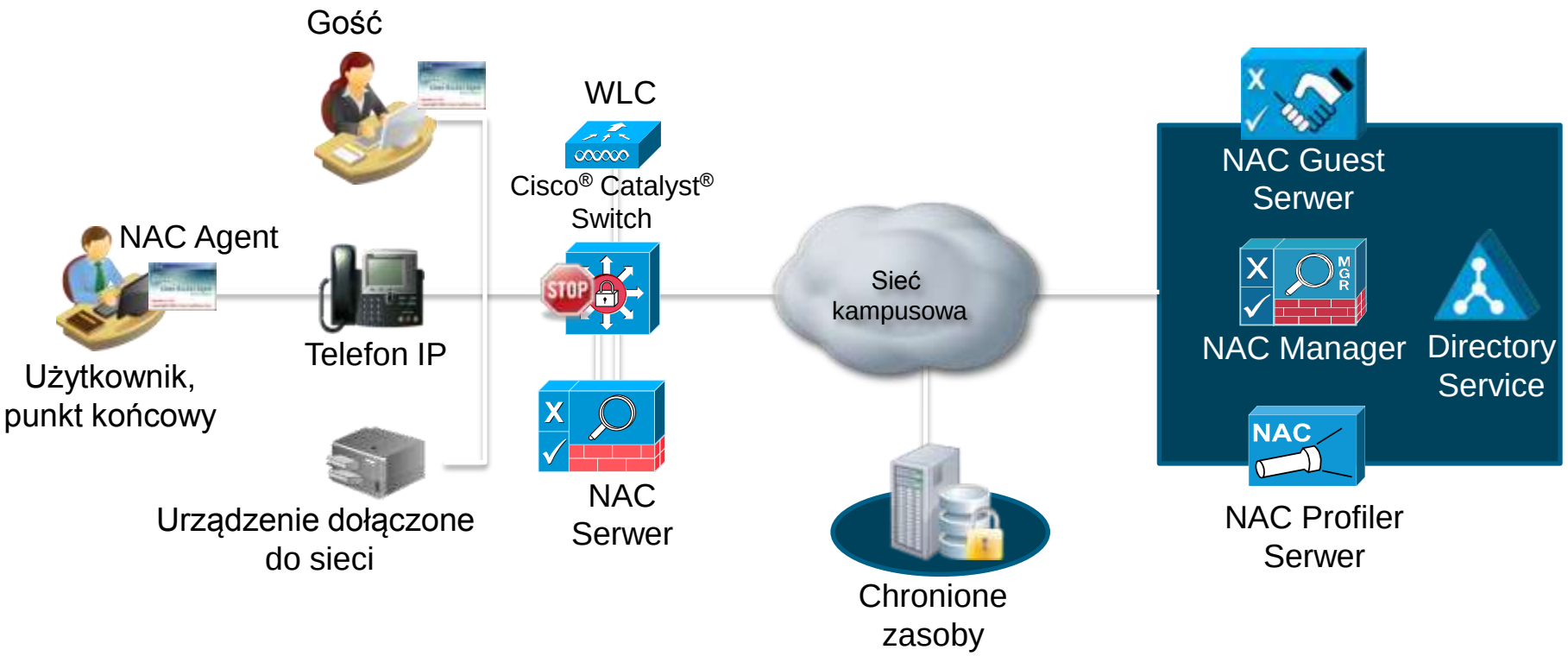


Warstwa kontrolna: **RADIUS**

ACS – Cisco Secure Access Control Server

Cisco TrustSec™

Kontrola dostępu w oparciu o NAC Appliance



Warstwa kontrolna: **SNMP**

802.1X i NAC Appliance - porównanie

	Cisco 802.1X	NAC Appliance
Wymagany agent lub suplikant?	Tak dla uwierzytelniania 802.1X. Nie dla uwierzytelniania przez WWW.	Agent wymagany dla SSO i oceny stanu maszyny (posture). Nie dla uwierzytelniania przez WWW.
Ocena stanu urządzenia	Nie*	Tak
Standard branżowy	Tak	Nie
Obsługa urządzeń bez suplikanta 802.1X	Tak – na bazie adresu MAC	Tak
Wsparcie dla urządzeń bez agenta	Tak: Profiler	Tak: Profiler
Wsparcie dla uwierzytelniania maszyn	Tak	Tak
Obsługa dostępu gościnnego	Tak	Tak
Protokół sterowania	RADIUS	SNMP

Uwierzytelnianie w oparciu o 802.1X

Cisco TrustSec™ - uwierzytelnianie w oparciu o 802.1X

1. IEEE 802.1X
   - Silna, zestandaryzowana metoda uwierzytelniania warstwy 2 dla użytkowników i urządzeń
2. MAC Authentication Bypass (MAB)
   - Urządzenia bez suplikanta 802.1X mogą być uwierzytelniane w oparciu o adres MAC lub profilowane automatycznie
3. WEB Authentication
   - Goście mogą korzystać z uwierzytelniania w oparciu o WWW w celu uzyskania ograniczonego dostępu do sieci

Cisco TrustSec™- elastyczność

Elastyczne uwierzytelnianie - trzy różne metody uwierzytelniania:

- 802.1X – dla urządzeń z suplikantem
- MAC Authentication Bypass (MAB)
- Web Authentication (typowo ID użytkownika / hasło)

Konfigurowane per port

- W dowolnej kombinacji
- W dowolnej kolejności

Redukuje koszty OPEX:

- Użytkownik może przenosić urządzenia bez interwencji administratora
- Brak zmian w sieci w momencie zmiany uwierzytelniania WWW na 802.1X

Elastyczne uwierzytelnianie (Flex-Auth)

Dowolna kombinacja
Dowolna sekwencja
Na pojedynczym porcie

Dostępne metody uwierzytelniania

802.1X | MAB | Web Auth

Uwierzytelnianie użytkowników

802.1X → MAB → Web Auth

Obsługa urządzeń

MAB → 802.1X → Web Auth

Web Authentication

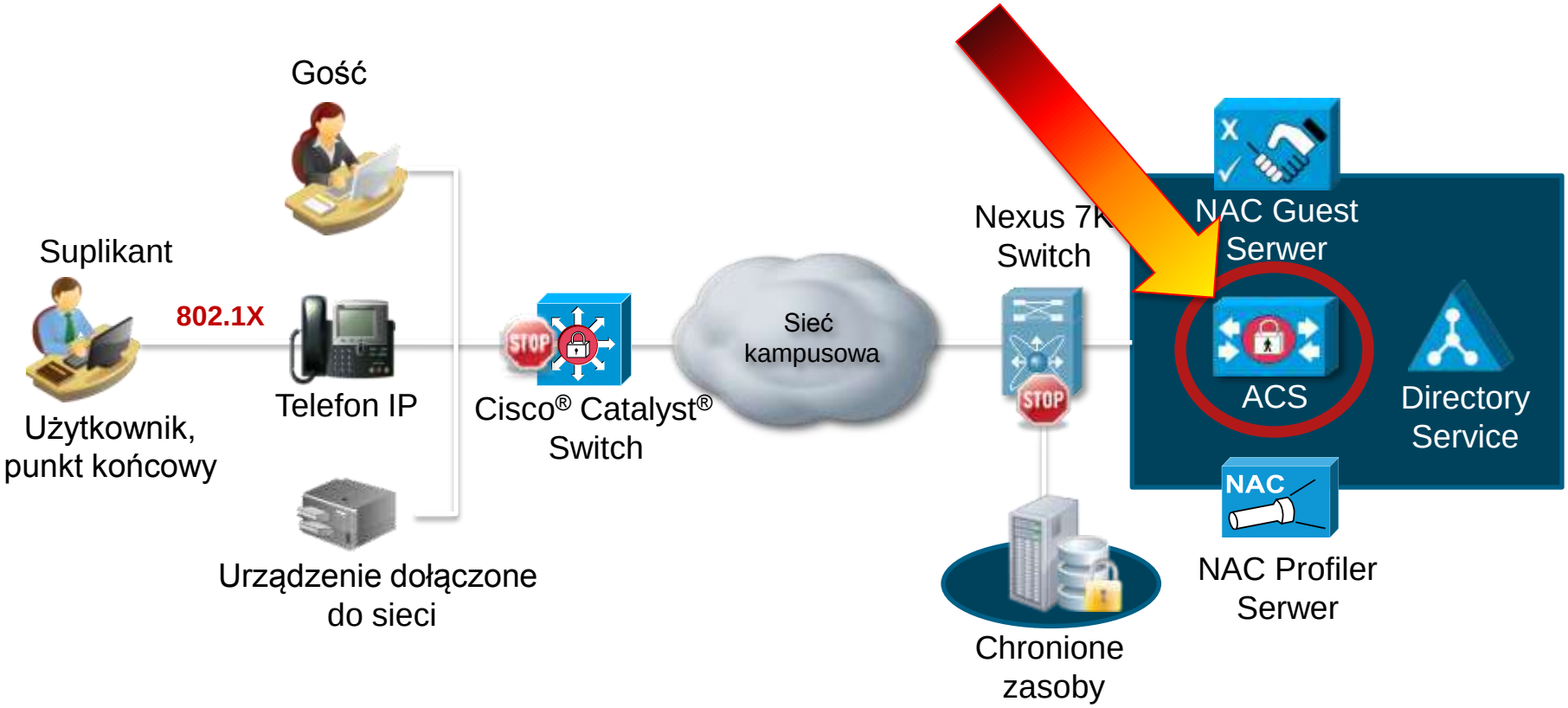
Web Auth → MAB

TrustSec: Autoryzacja i polityki w sieci

Różne mechanizmy autoryzacji

- TrustSec™ oferuje różnorodne mechanizmy autoryzacji w zakresie egzekwowania polityki
- Trzy główne mechanizmy wdrażania polityki/segmentacji:
  - Dynamiczne **przypisanie VLAN** – Ingress
  - Dynamiczna **lista ACL** – Ingress
  - Security Group Access Control List (**SGACL**) - Egress
- Trzy różne tryby egzekwowania polityki:
  - Monitor Mode
  - Low Impact Mode (z pobieraną per sesja listą ACL)
  - High-Security Mode

Cisco TrustSec™ - autoryzacja i punkty wdrażania polityk



Warstwa kontrolna: **RADIUS**

System uwierzytelniania: ACS 5.2

Cisco Secure Access Control System 5.2

Dostępne „smaki”

Sprzętowy system 1121

- Dedykowany serwer 1RU

Wirtualny system VMware

- Gotowy obraz systemu dla VMware ESX 3.5 lub 4.0

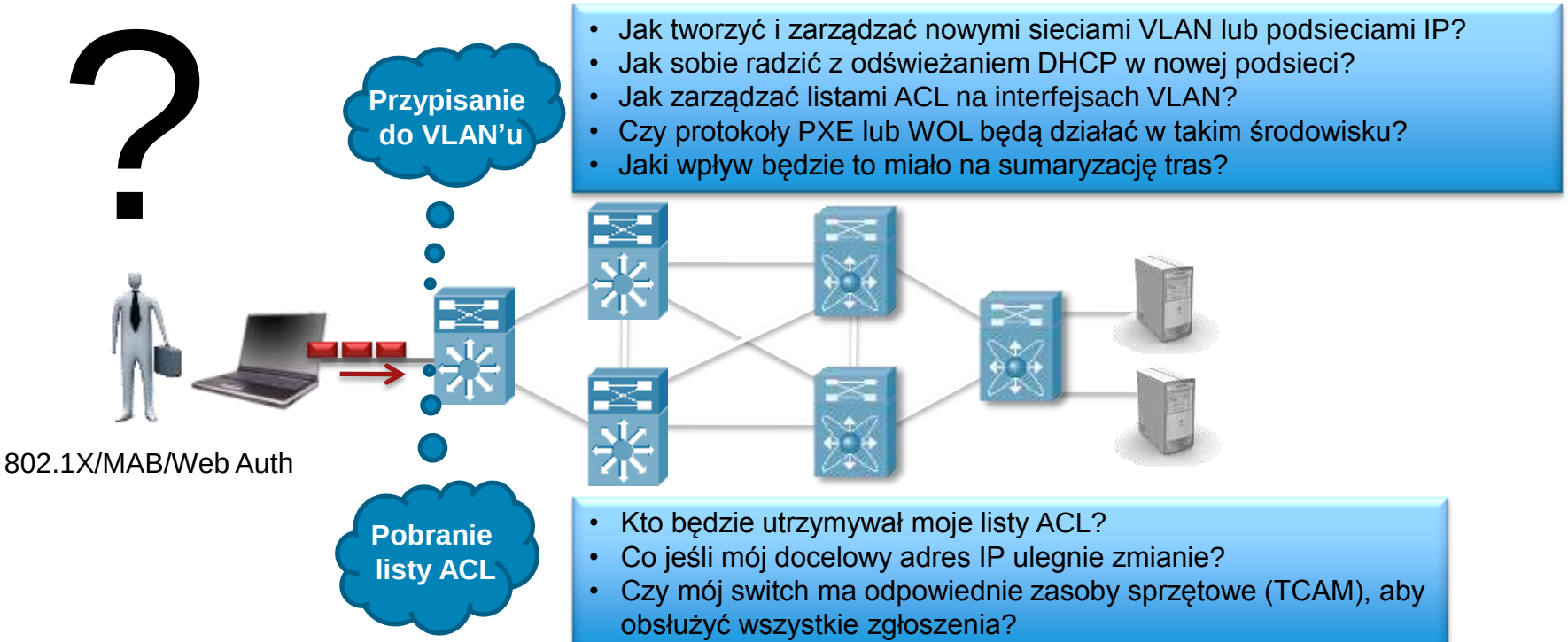
Wersja 5.2 wprowadza

Internet Explorer 8 dla interfejsu zarządzania

Integrację AD z Windows 2008 R2

SHA-256

Kontrola dostępu na wejściu



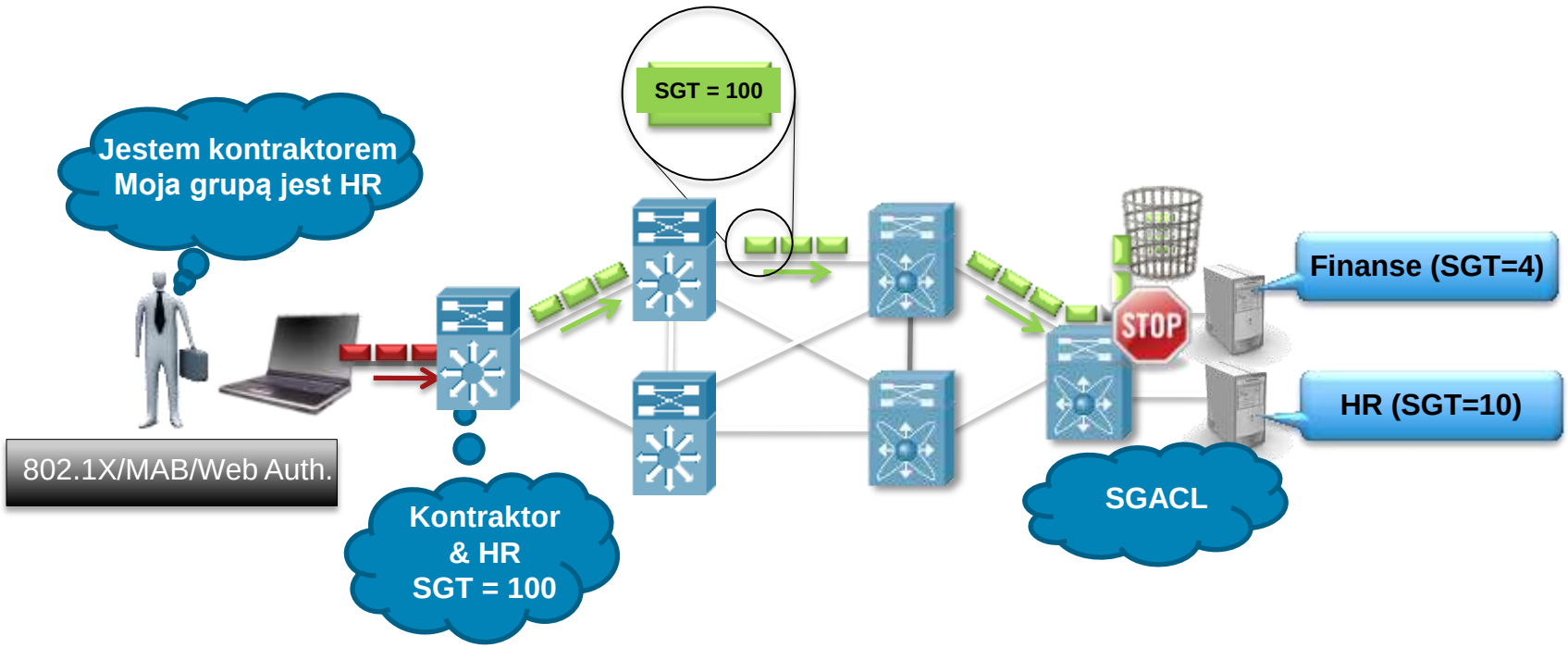
- Jak tworzyć i zarządzać nowymi sieciami VLAN lub podsieciami IP?
- Jak sobie radzić z odświeżaniem DHCP w nowej podsieci?
- Jak zarządzać listami ACL na interfejsach VLAN?
- Czy protokoły PXE lub WOL będą działać w takim środowisku?
- Jaki wpływ będzie to miało na sumaryzację tras?

- Kto będzie utrzymywał moje listy ACL?
- Co jeśli mój docelowy adres IP ulegnie zmianie?
- Czy mój switch ma odpowiednie zasoby sprzętowe (TCAM), aby obsłużyć wszystkie zgłoszenia?

Tradycyjne metody autoryzacji posiadają pewne ograniczenia:

- Wymagany jest szczegółowy projekt przed wdrożeniem w przeciwnym razie…
- Nie są tak elastyczne jak wymaga tego dzisiejsze środowisko sieciowe
- Projekt kontroli dostępu kończy się przebudową całej sieci

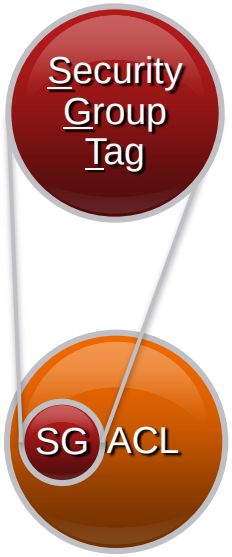
TrustSec: Security Group Access (SGA)



Security Group Access pozwalają:

- Utrzymać istniejący schemat logiczny w warstwie dostępowej
- Stosować polityki spełniające wymagania dzisiejszych sieci
- Rozpowszechniać polityki z centralnego serwera zarządzania

Security Group Access (SGA)



- **Unikalny** znacznik przypisywany do **unikalnej roli (zasobu)**
- Reprezentuje **przywileje użytkownika/urządzenia źródłowego**
- **Znakowany na wejściu** do domeny TrustSec™

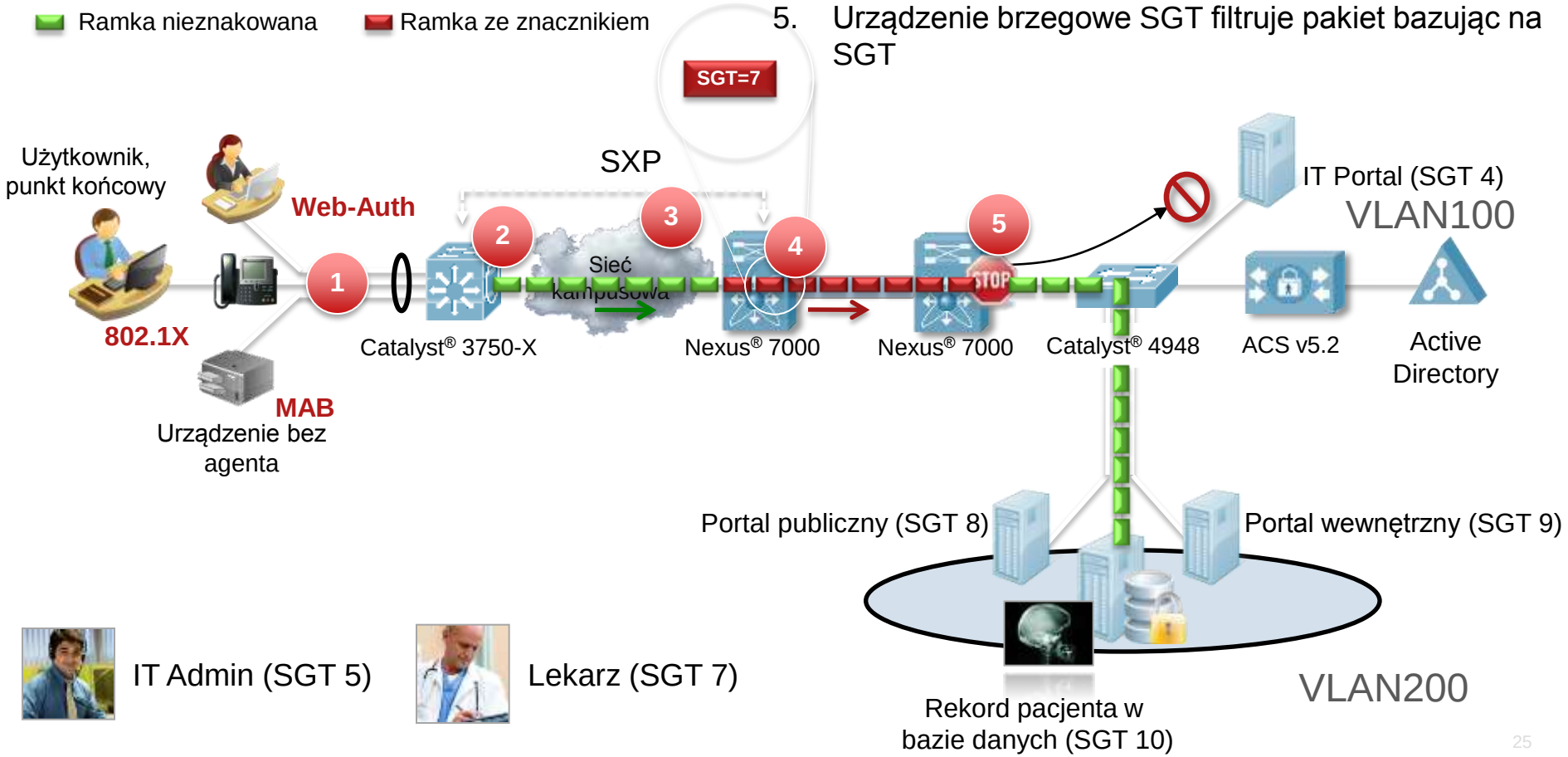
- **Filtrowanie (SGACL) na wyjściu** z domeny TrustSec™
- **Adres IP nie jest wymagany w ACE** (adres IP powiązany z SGT)
- Polityka (ACL) jest **dystrybuowana z centralnego serwera (ACS)** lub konfigurowana lokalnie na urządzeniu TrustSec™

Korzyści

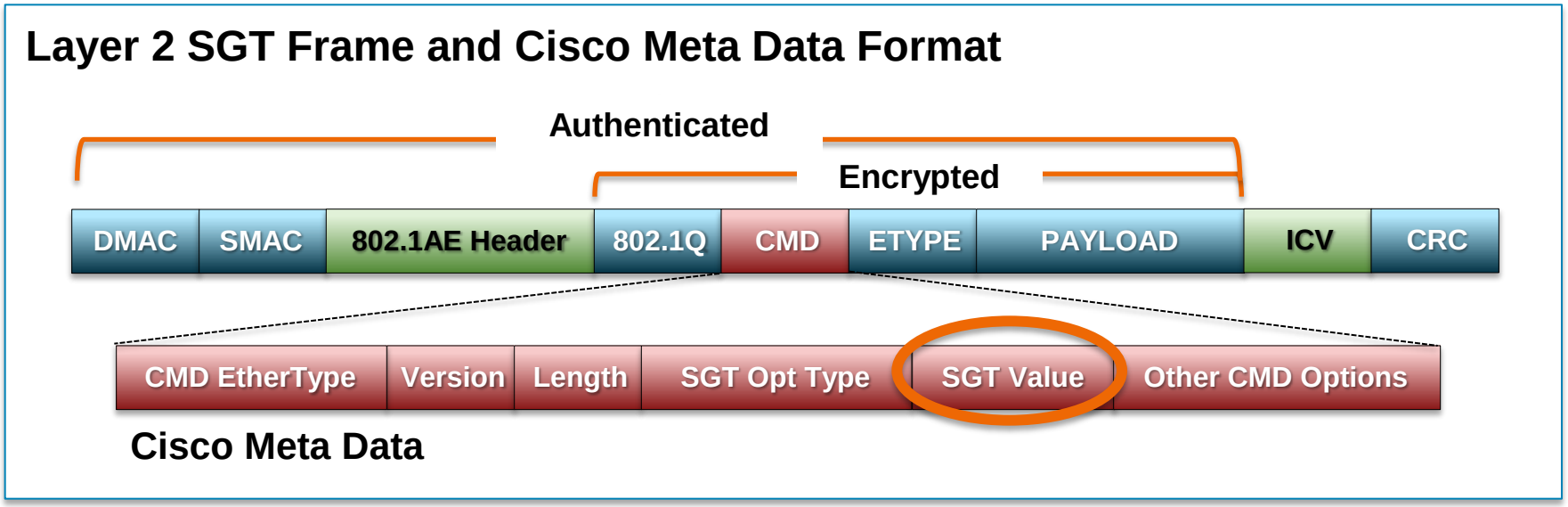
- Zapewnia politykę **niezależną od topologii**
- Elastyczność i skalowalność polityki opartej na roli użytkownika
- **Scentralizowane zarządzanie politykami** w celu dynamicznego wdrażanie polityk
- Filtrowanie na wyjściu **redukuje zużycie zasobów TCAM**

Kontrola dostępu w oparciu o SGA jak to działa?

1. Punkt końcowy dołączony do sieci
2. Switch uwierzytelnia użytkownika i przypisuje SGT
3. SXP wiąże IP-do-SGT i uzupełnia tabelę powiązań N7K
4. Urządzenie brzegowe SGT odbiera pakiet i wstawia SGT
5. Urządzenie brzegowe SGT filtruje pakiet bazując na SGT



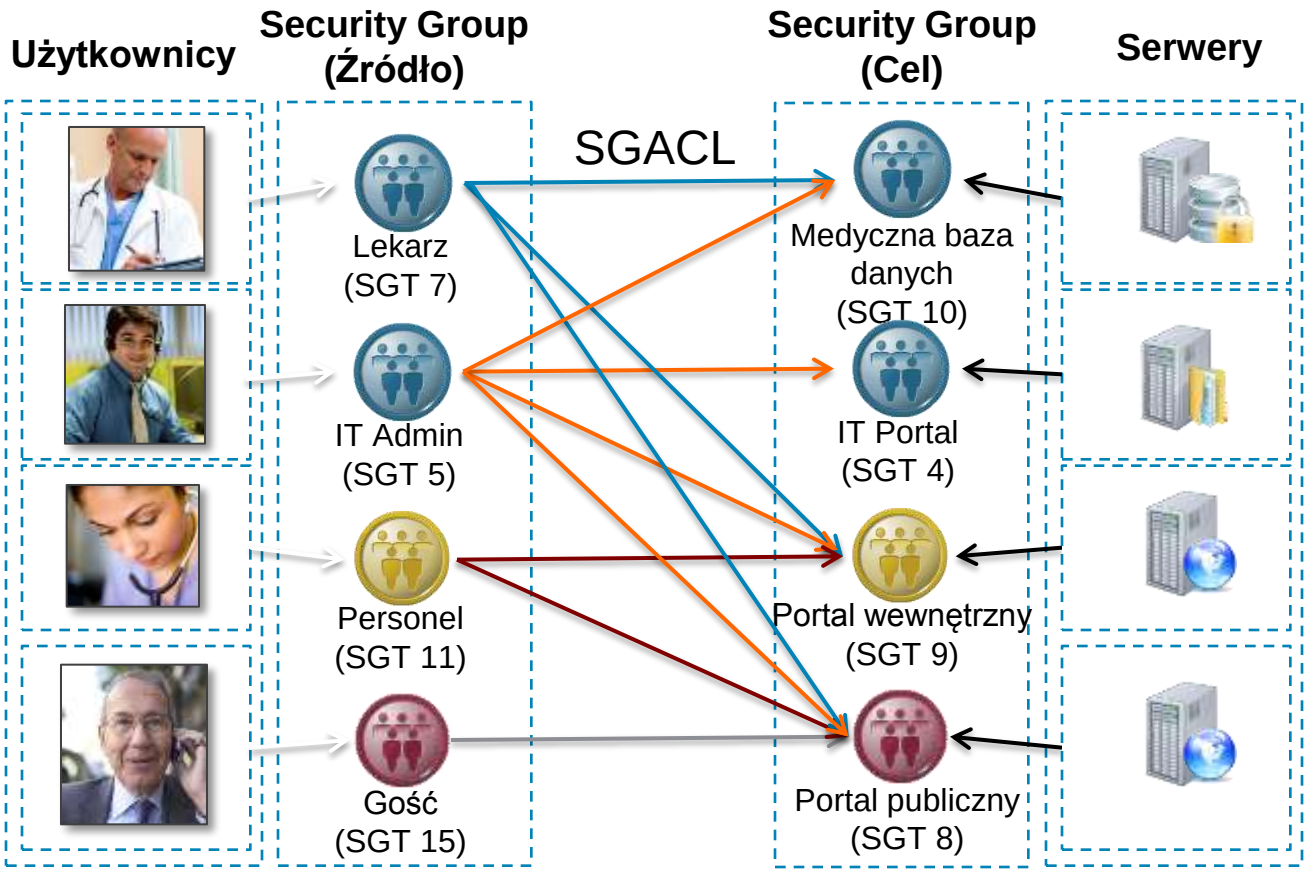
Layer 2 SGT Frame Format



- 802.1AE Header | CMD | ICV are the L2 802.1AE + TrustSec overhead (=~40bytes)
- Tagging process prior to other L2 service such as QoS
- SGT namespace is managed on central policy server (ACS 5.x)
- No impact IP MTU/Fragmentation.

Normal Ethernet Frame

Jak SGA upraszcza kontrolę dostępu
Model



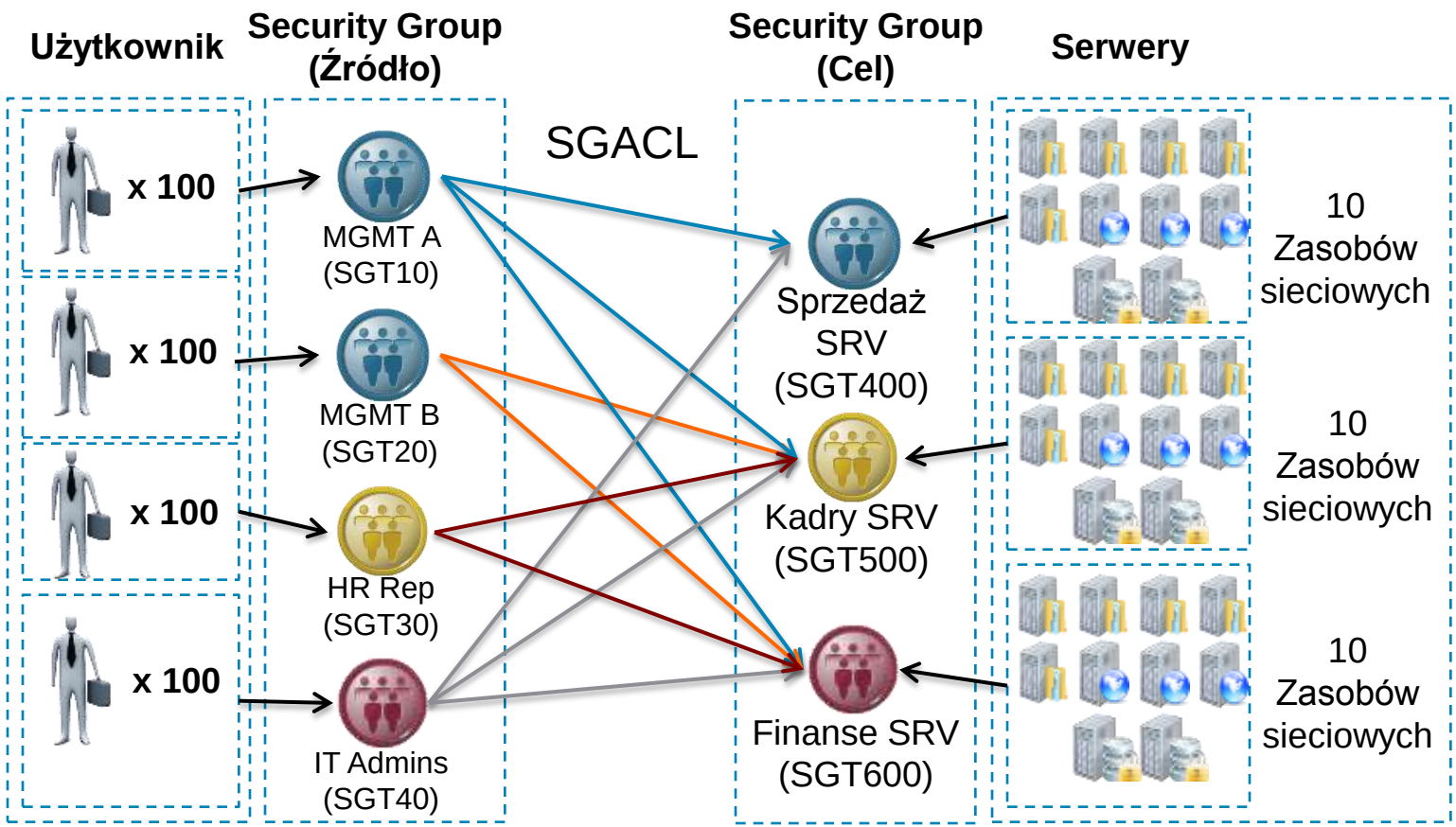
SGACL – reguły dostępu

SGT celu / SGT źródła	Portal publiczny (SGT 8)	Portal wewnętrzny (SGT 9)	IT Portal (SGT 4)	Medyczna baza danych (SGT 10)
 Lekarz (SGT 7)	www	www	Brak dostępu	www Udostępnianie plików
 IT Admin (SGT	www SSH RDP Udostępnianie plików		Pełny dostęp	SSH RDP Udostępnianie plików

ACL_DLA_DZIALU_IT

```
permit tcp dst eq 443
permit tcp dst eq 80
permit tcp dst eq 22
permit tcp dst eq 3389
permit tcp dst eq 135
permit tcp dst eq 136
permit tcp dst eq 137
permit tcp dst eq 138
permit tcp des eq 139
deny ip
```

Jak SGACL upraszcza kontrolę dostępu
Przykład rzeczywisty



Jak SGACL upraszcza kontrolę dostępu
Liczymy

400 użytkowników

30 zasobów sieciowych

Tylko cztery definicje protokołów/portów

Tradycyjny ACL na interfejsie VLAN – używamy zakresów dla sieci źródłowych

4 VLANy (src) * 30 (dst) * 4 uprawnienia = **480 wpisów**

Dynamiczny ACL (dACL)

1 Grupa (src) * 30 (dst) * 4 uprawnienia = **120 wpisów**

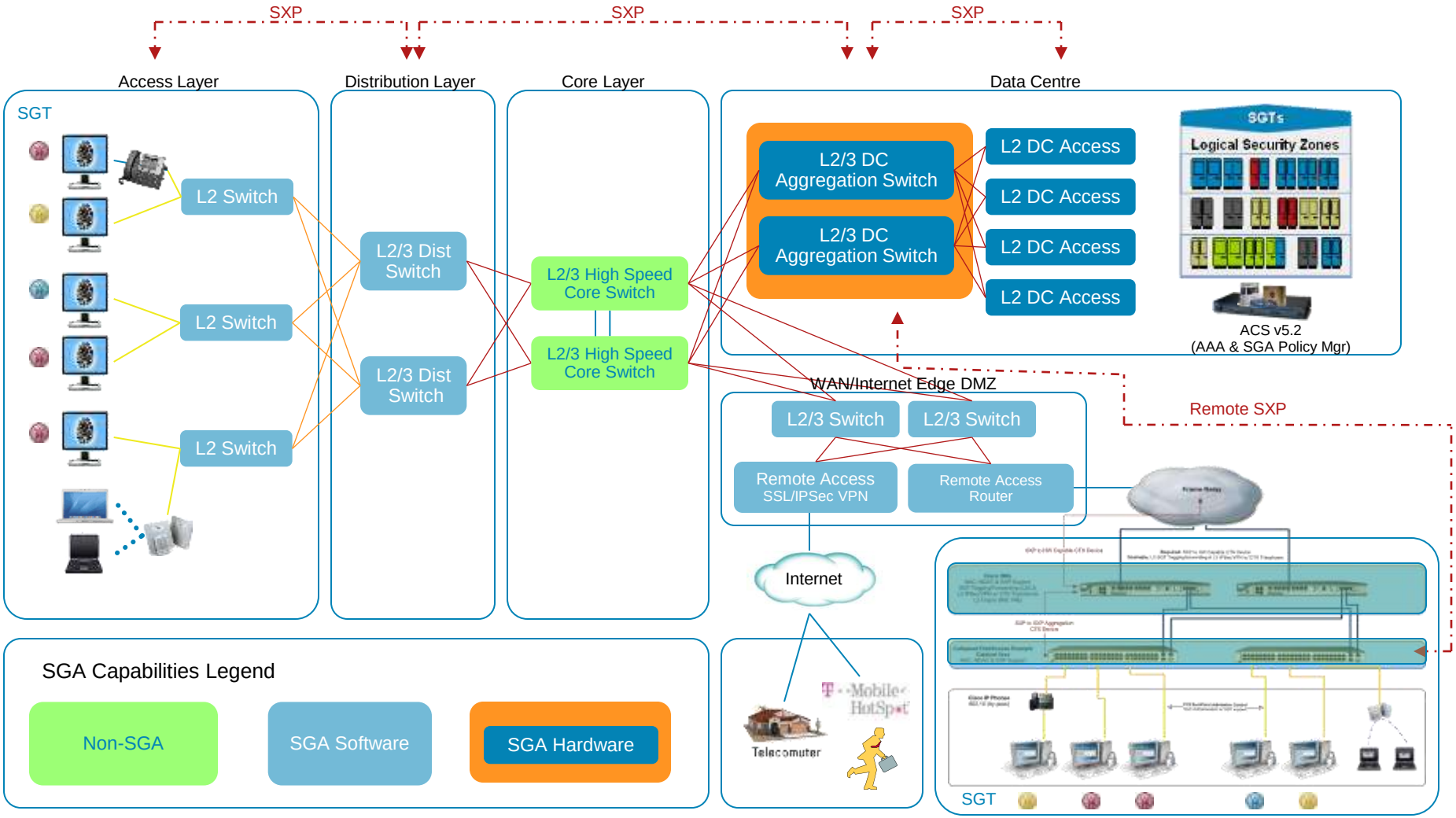
TrustSec za pomocą SGACL

4 SGT (src) * 3 SGT (dst) * 4 uprawnienia = **48 wpisów**

Cisco TrustSec: Co dalej?

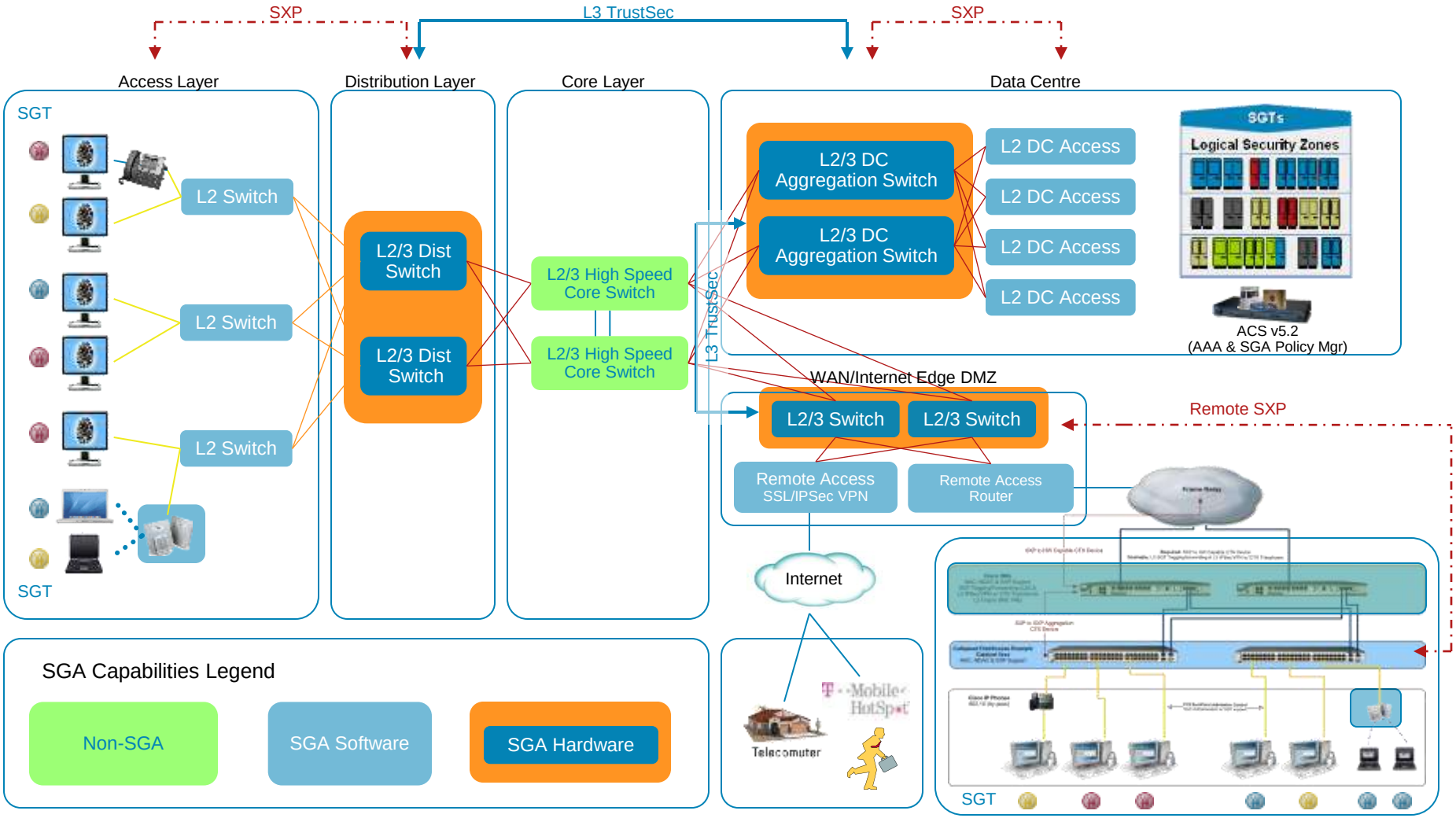
Ewolucja SGA

Faza 1



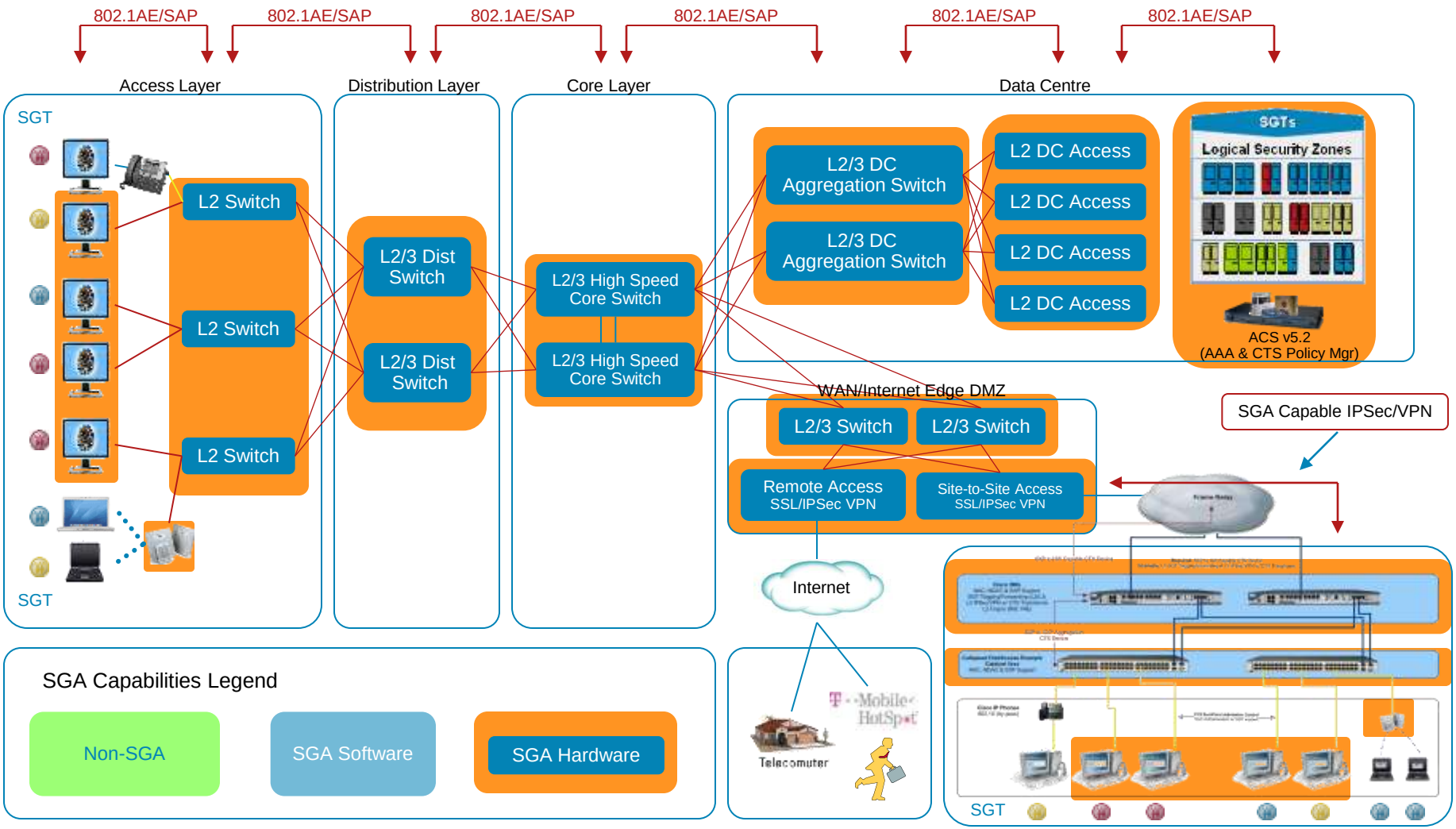
Ewolucja SGA

Faza 2



Ewolucja SGA

Faza 3



TrustSec: Integralność i poufność danych

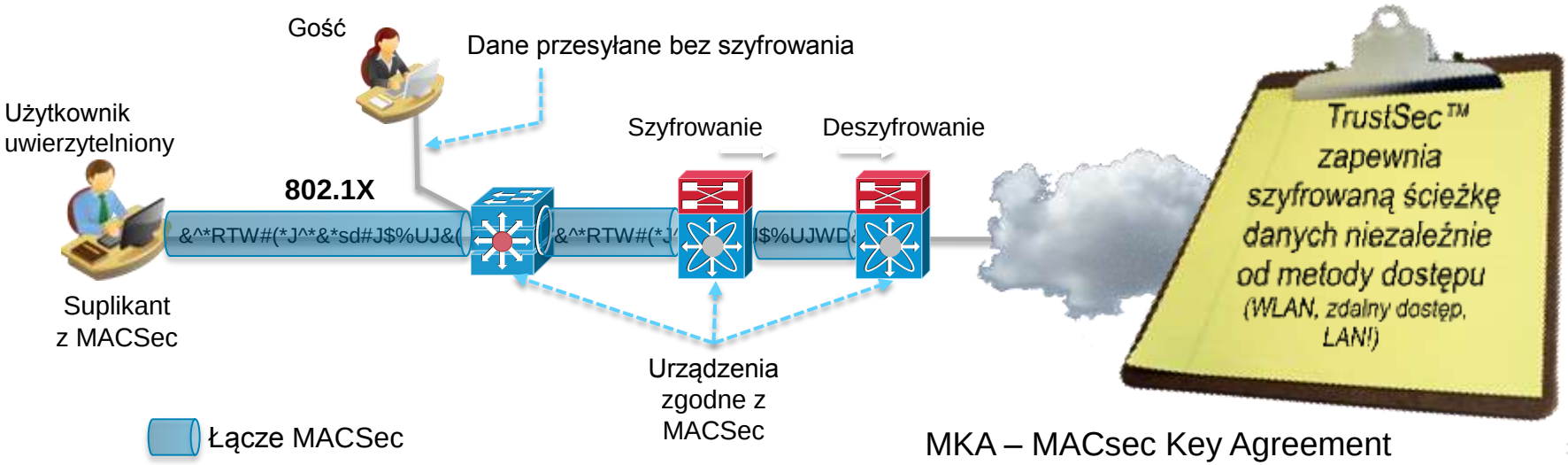
Poufność i integralność danych MACSec

802.1AE

Media Access Control Security (MACSec)

- Zapewnia szyfrowanie “równoważne zabezpieczeniom w sieciach WLAN / VPN” (128-bitowy AES GCM) dla połączeń LAN
- Zaaprobowane przez NIST* szyfrowanie (IEEE802.1AE) + zarządzanie kluczami (IEEE802.1X-2010/MKA)
- Umożliwia realizację standardowych usług bezpieczeństwa

* National Institute of Standards and Technology (USA) – dokument 800-38D



MAC Sec – obsługiwane urządzenia

802.1AE

MACSec na brzegu sieci

- Catalyst® 3750X/3560X (porty dostępowe)
- Wymagane oprogramowanie Cisco IOS® 12.2(53)SE2
- 802.1X-REV (MKA) dla zarządzania kluczami

MACSec dla infrastruktury

- Przełączniki Nexus® 7000
- Obsługiwane karty liniowe 1GbE/10GbE
- Wymagane oprogramowanie NX-OS 5.0(2)a
- Security Association Protocol (SAP - protokół Cisco) dla zarządzania kluczami

Uwaga: Zarówno SAP, jak i MKA wymaga ACS 5.1 lub wersji późniejszej. SAP posiada opcję statycznej konfiguracji kluczy na interfejsach Nexus 7000. Obecnie MACSec/MKA jest używane na brzegu sieci, a MACSec/SAP na połączeniach między przełącznikami. W przyszłości MACSec/MKA (Standard) będzie obsługiwany w całej sieci.

AnyConnect 3.0 z obsługą MACSec

802.1AE

AnyConnect 3.0 umożliwia

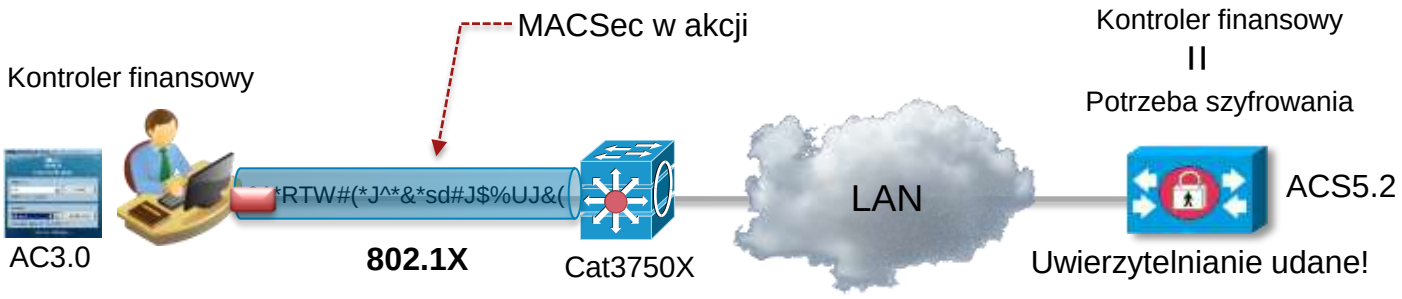
- Wspólny interfejs dla sieci SSL-VPN, IPSec i 802.1X dla połączeń LAN / WLAN
- Obsługę MACSec / MKA (802.1X-REV) dla programowego szyfrowania danych (wydajność zależna od CPU punktu końcowego)
- Karty z obsługą sprzętową MACSec umożliwiają zwiększenie wydajności z AnyConnect 3.0 ☺

Karty ze sprzętową obsługą MACSec:

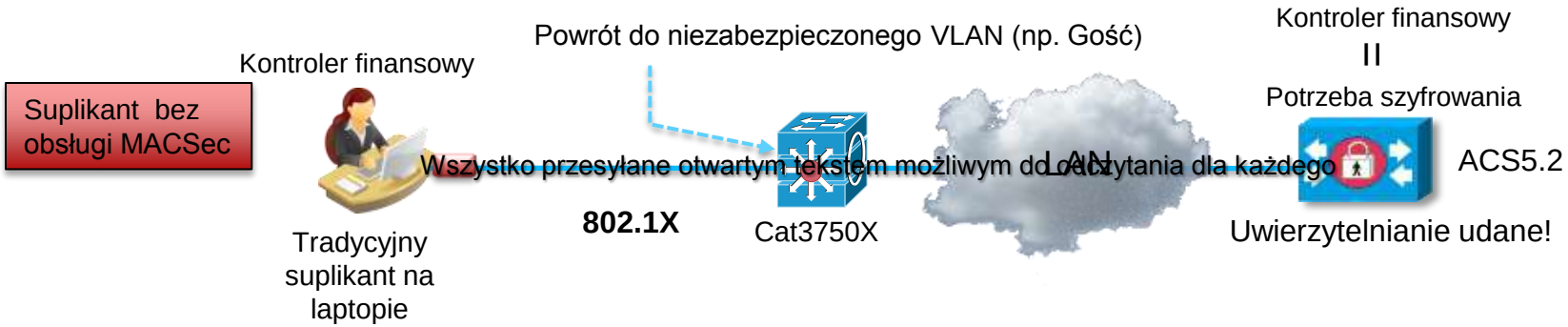
Intel 82576 Gigabit Ethernet Controller
Intel 82599 10 Gigabit Ethernet Controller
Intel ICH10 - Q45 Express Chipset (1Gbe LOM)
(Dell, Lenovo, Fujitsu i HP posiadają w ofercie komputery z tym układem LOM)

Polityka szyfrowanie przy użyciu MACSec

Z wykorzystaniem AnyConnect 3.0



Z wykorzystaniem tradycyjnego suplikanta

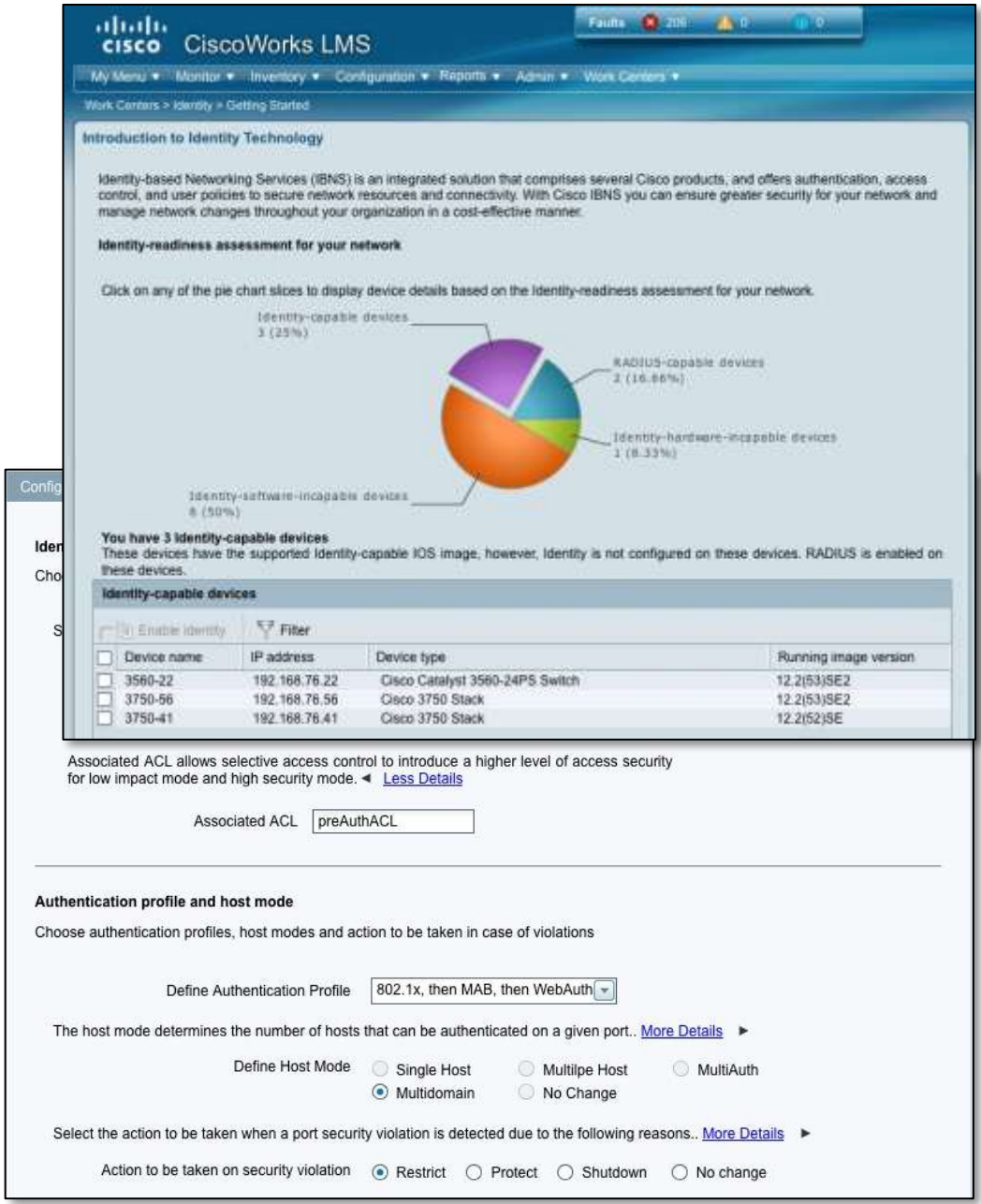


Monitoring i zarządzanie

CiscoWorks LMS 4.0 integruje TrustSec™

TrustSec™ Identity Work Center

- Oferuje najlepsze praktyki wdrożeniowe na podstawie dokumentów Cisco Validated Design (CVD)
- Zawiera profile uwierzytelniania z rozszerzeniami Cisco (Flex-Auth itp.)
- Posiada możliwość sprawdzenia gotowości do wdrożenia TrustSec™ (wizard)
- Konsola (Dashboard) dający wgląd w trendy uwierzytelniania i autoryzacji aktualnie w naszej sieci



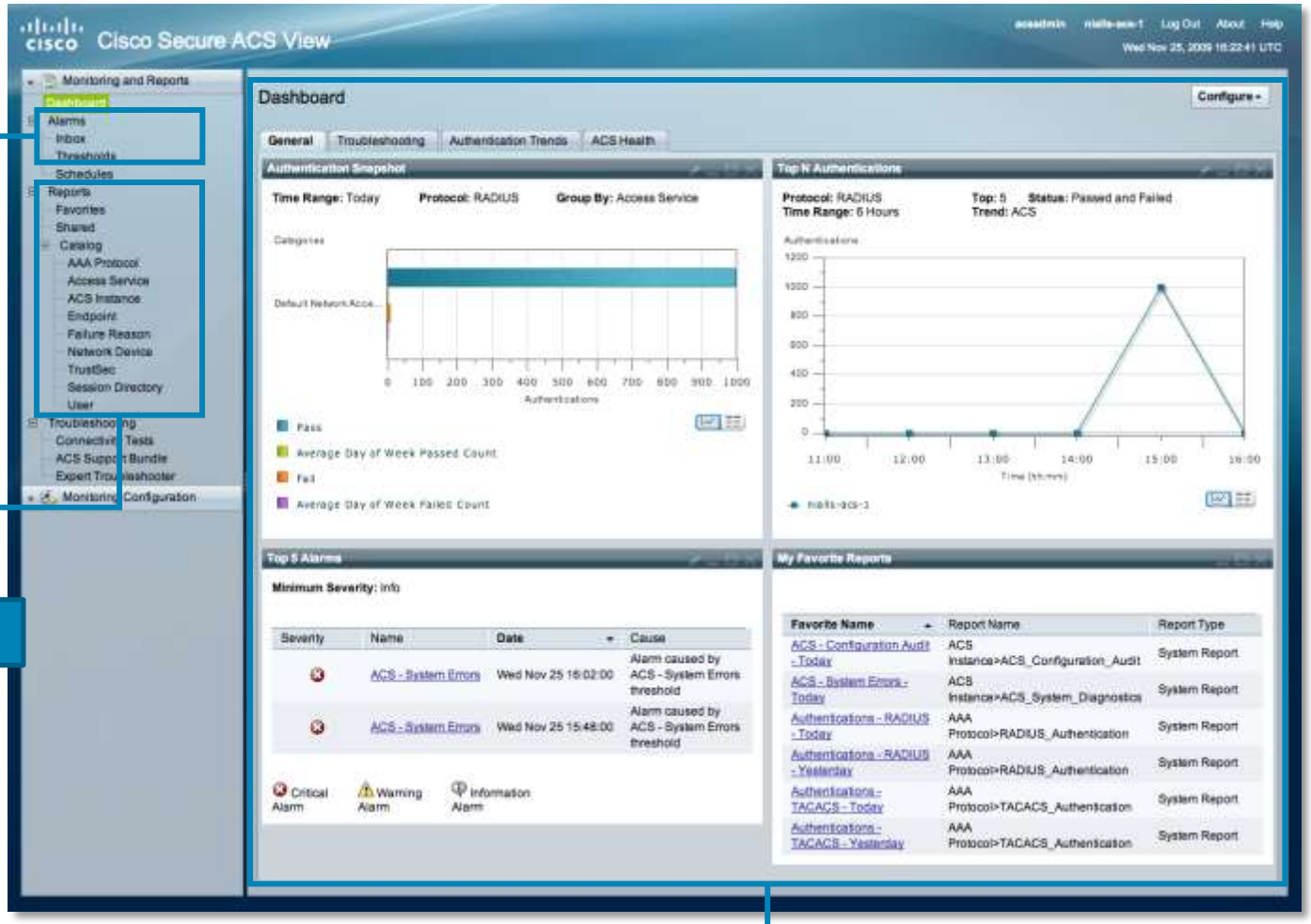
Cisco ACS
Monitoring & Troubleshooting Tool

Alarmy i powiadomienia

- Parametryzacja wyzwalania
- Powiadomienia e-mail i syslog

Bogate raportowanie

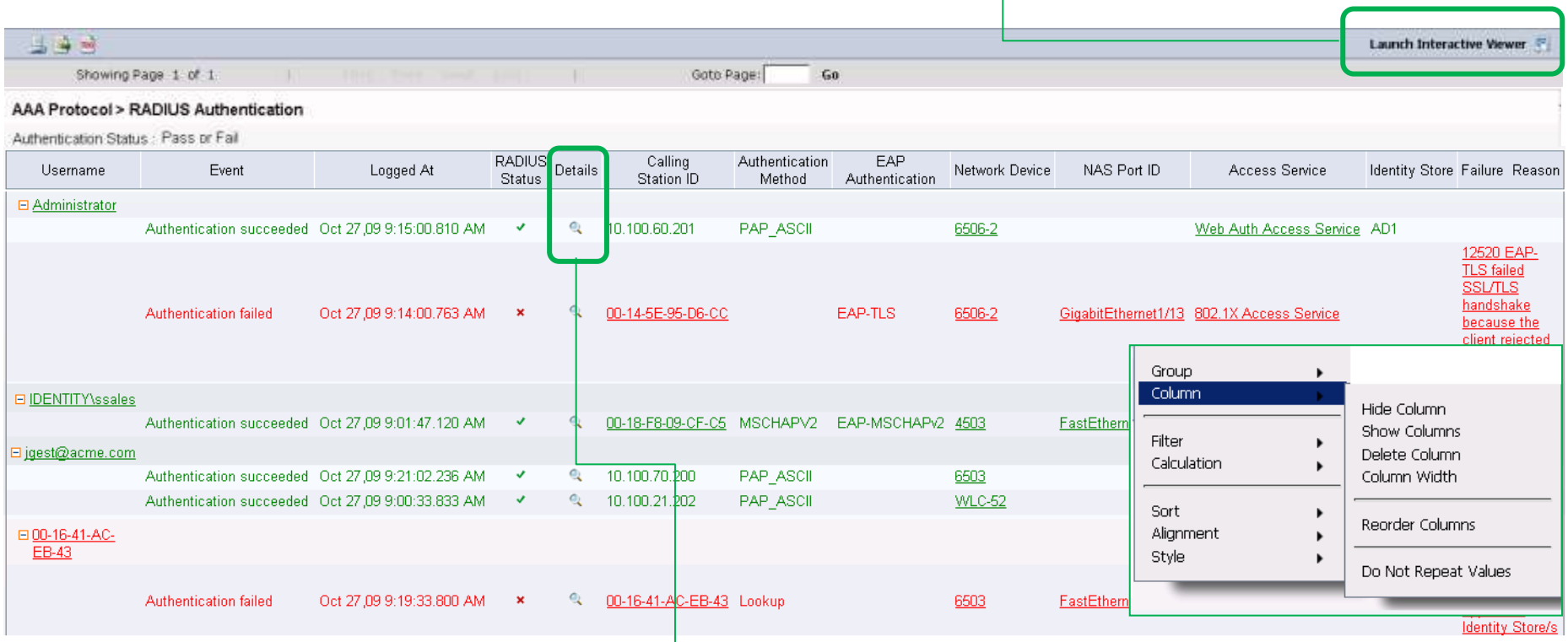
- Raporty
- Wzory
- Parametryzacja



Konfigurowalna konsola

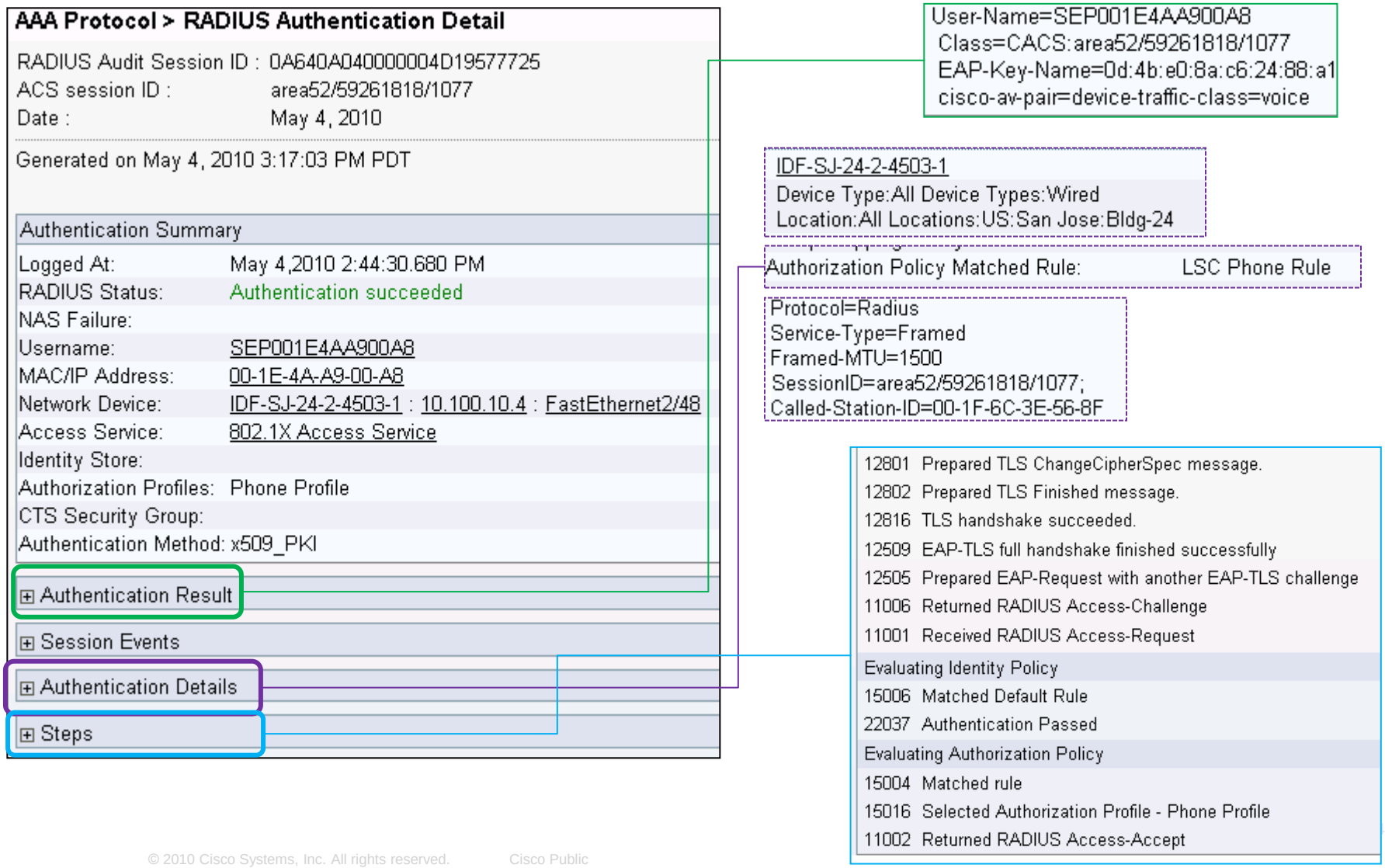
Monitorowanie w ACS 5.2

Ciekawostka: „*Interactive Viewer*” twoim przyjacielem



Dokładne raporty często ratują z opresji

ACS 5.2 Dokładne raporty



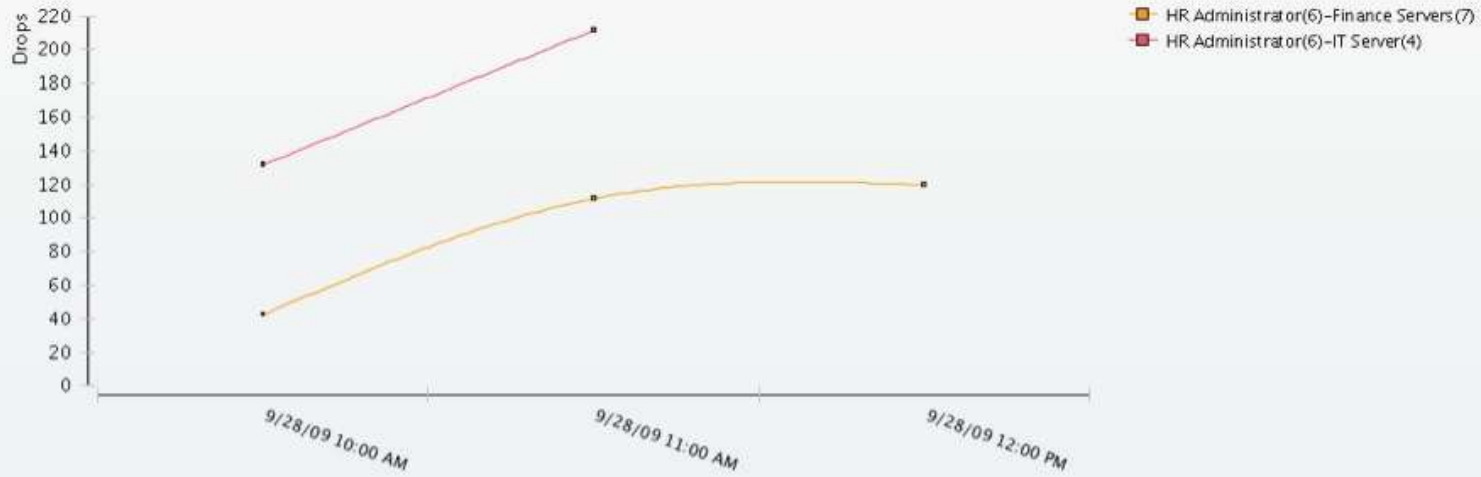
Monitorowanie działania SGACL

TrustSec > RBACL Drop Summary

Date : September 28, 2009

Generated on : September 28, 2009 2:12:09 PM PDT

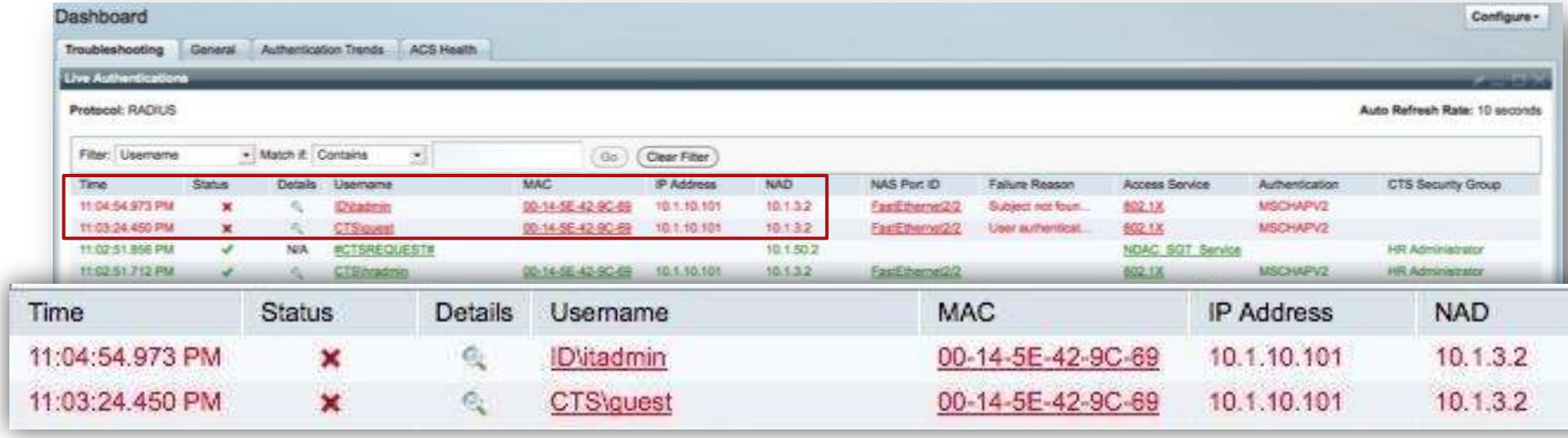
Reload



Time	Drops	User	Src Address	Src Port	Destination	Dest Address	Dest Port	Protocol	SGACL	SGT	DGT
September 28 10:00:00 AM											
	43	CTS\hradmin	10.1.10.100	20134		10.1.200.300	80	tcp (6)	Deny IP, Permit IP	HR Administrator(6)	Finance Servers(7)
	132	CTS\hradmin	10.1.10.100	20134		10.1.200.200	80	tcp (6)	Permit IP	HR Administrator(6)	IT Server(4)
September 28 11:00:00 AM											
	112	CTS\hradmin	10.1.10.100	20134		10.1.200.300	80	tcp (6)	Deny IP, Permit IP	HR Administrator(6)	Finance Servers(7)
	212	CTS\hradmin	10.1.10.100	20134		10.1.200.200	80	tcp (6)	Permit IP	HR Administrator(6)	IT Server(4)
September 28 12:00:00 PM											
	120	CTS\hradmin	10.1.10.100	20134		10.1.200.300	80	tcp (6)	Deny IP, Permit IP	HR Administrator(6)	Finance Servers(7)

Konsola uwierzytelniania – na żywo!

1. „Dashboard Live Authentication Log” umożliwia szybki dostęp do informacji uwierzytelniania w czasie rzeczywistym.
2. Zagłębianie się z poziomu konsoli umożliwia dotarcie do bardziej szczegółowych informacji. Wszystko z jednego miejsca!



Time	Status	Details	Username	MAC	IP Address	NAD
11:04:54.973 PM	✖		ID\tadmin	00-14-5E-42-9C-69	10.1.10.101	10.1.3.2
11:03:24.450 PM	✖		CTS\guest	00-14-5E-42-9C-69	10.1.10.101	10.1.3.2

Cisco TrustSec

1. TrustSec to architektura, której celem jest realizacja wizji sieci bez granic, w szczególności mobilności użytkownika – sieć musi wiedzieć kim jest użytkownik, aby przyznać mu odpowiednie prawa dostępu niezależnie od tego, gdzie on się znajduje
2. Centralizacja kontroli bezpieczeństwa
3. Zachowanie pełnej kontroli nad siecią - to dlatego 802.1AE jest częścią TrustSec – szyfrowanie „end-to-end” uniemożliwiłoby zastosowanie mechanizmów klasyfikacji i filtracji ruchu

NAC Appliance – o tym po przerwie 15 minut

cisco.com/go/trustsec