

Novell Access Manager

Dostęp przez przeglądarkę do firmowych aplikacji
webowych i tradycyjnych (SSL VPN)

Dariusz Leonarski
Starszy konsultant
dleonarski@novell.pl

Novell Sp. z o.o.

Novell[®]



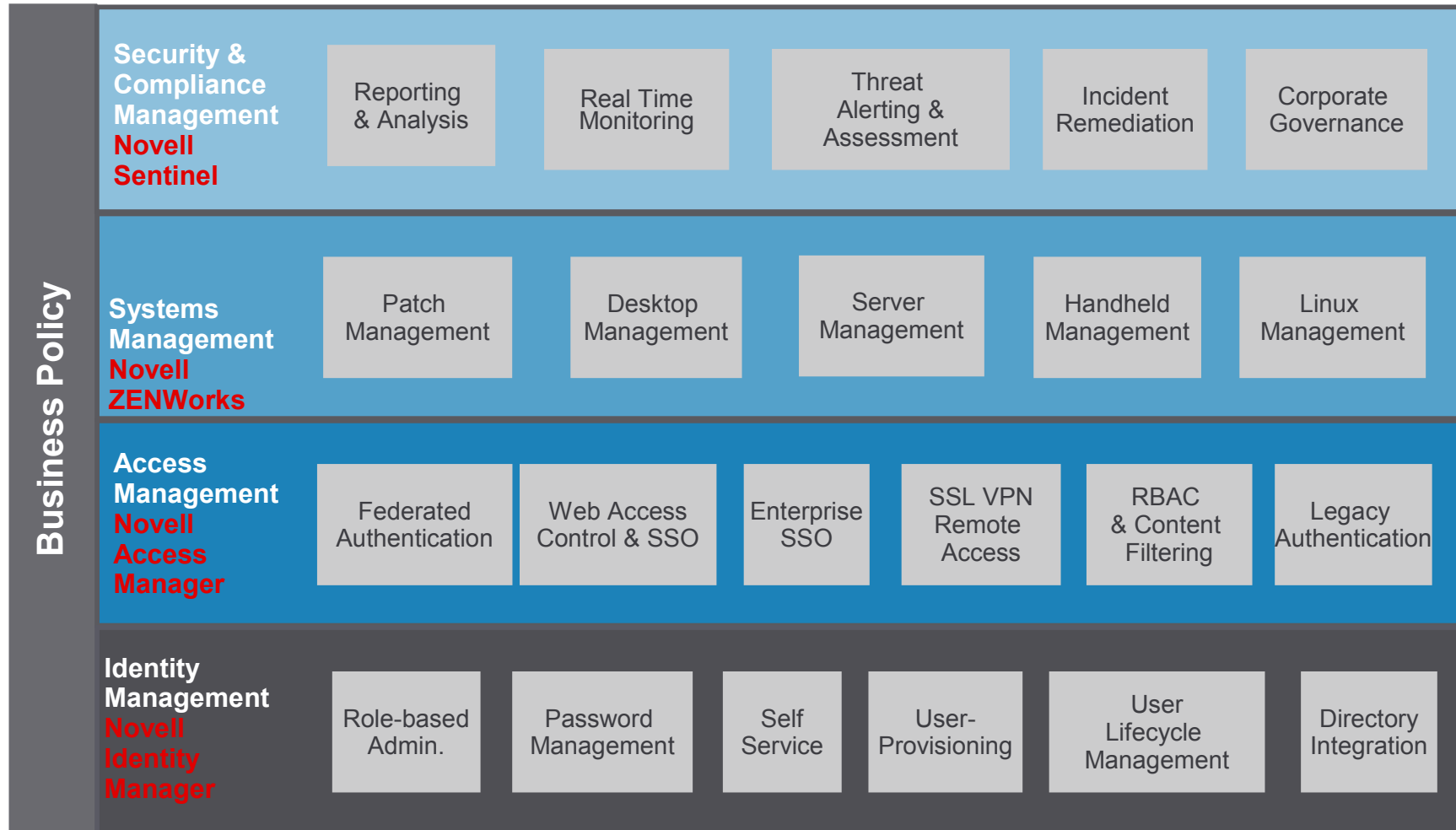
Bogactwo różnych opcji

Trudne do określenia priorytetów i właściwej drogi do sukcesu





Kompletne portfolio rozwiązań Identity & Security



Novell liderem rozwiązań bezpieczeństwa

Wyróżnione produkty:
 Identity Manager
 Access Manager
 SecureLogin
 Sentinel

Figure 1. Magic Quadrant for Enterprise Single Sign-On, 2007

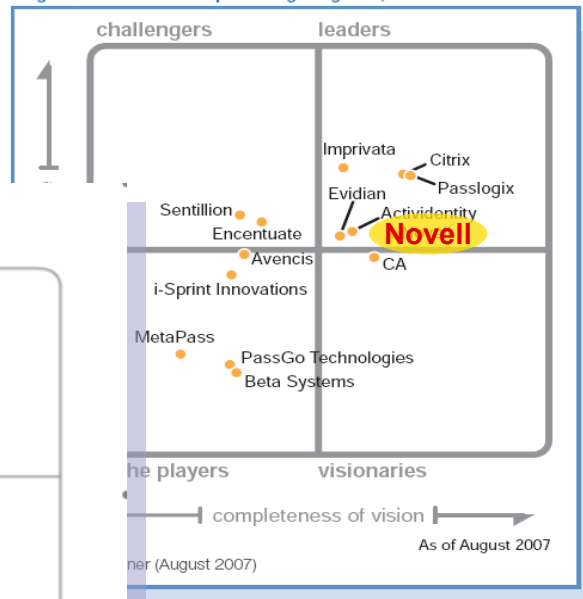


Figure 1. Magic Quadrant for User Provisioning, 2H07

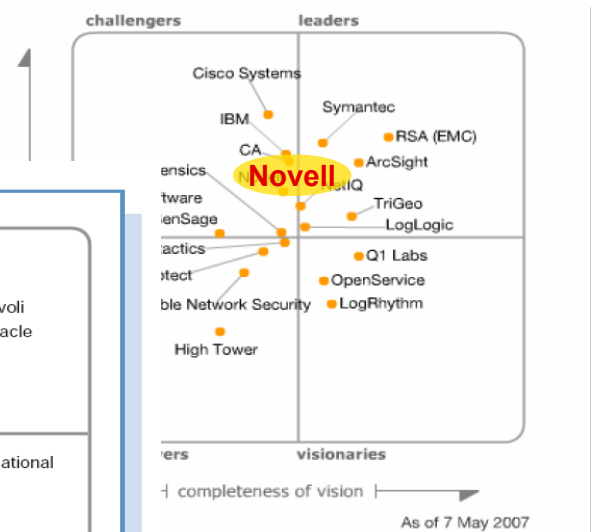
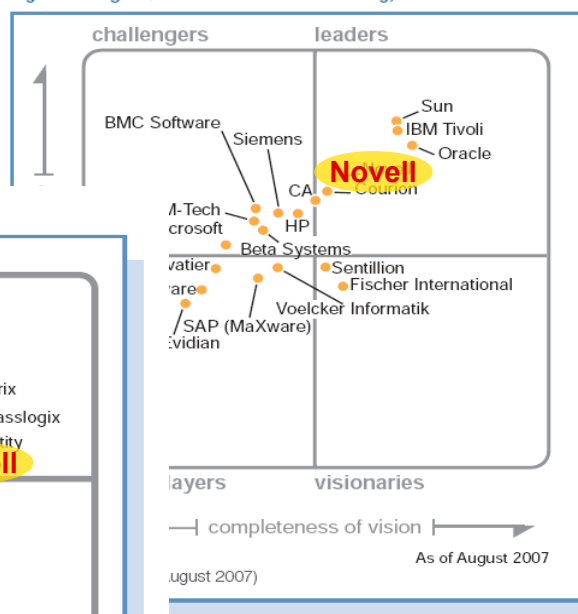
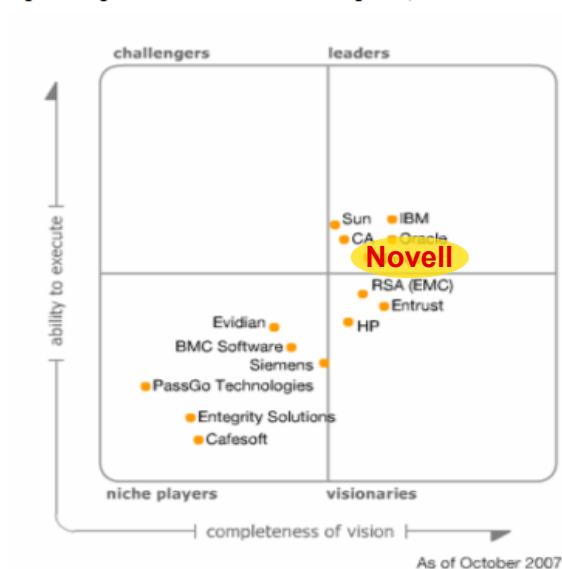


Figure 1. Magic Quadrant for Web Access Management, 2H07



Source: Gartner (October 2007)

Gartner

The background of the slide is a solid blue color with a pattern of diagonal lines in a lighter shade of blue, creating a sense of motion or depth.

Novell Access Manager 3.1

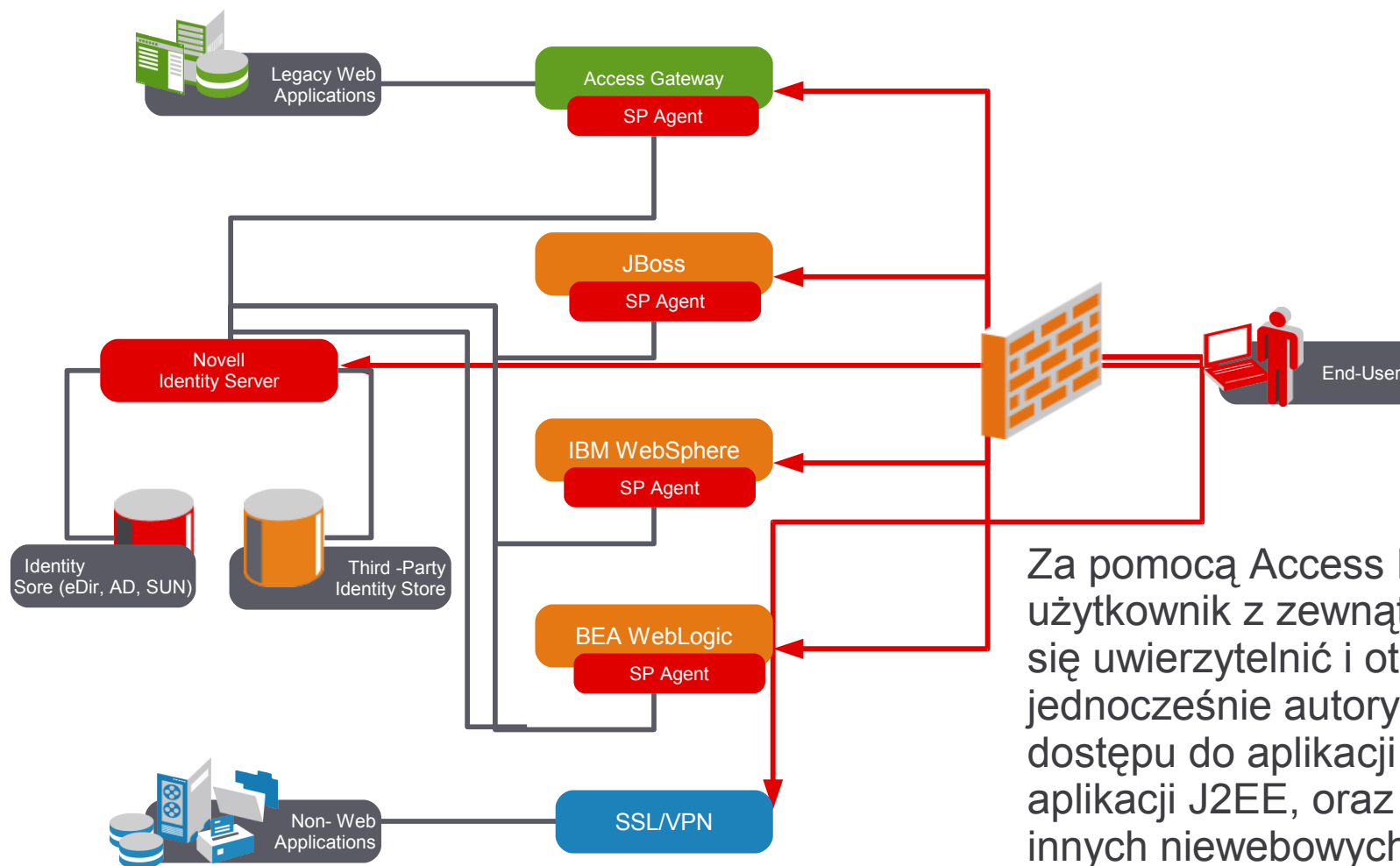
zarządzanie dostępem

Novell Access Manager

Obszerna, oparta o tożsamość kontrola bezpieczeństwa i dostępu



Novell Access Manager

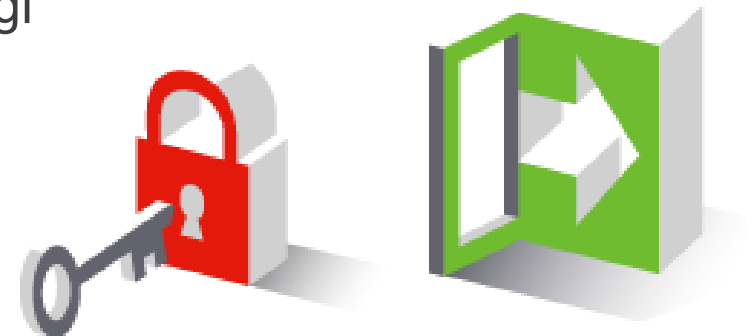


Za pomocą Access Managera użytkownik z zewnątrz może raz się uwierzytelnić i otrzymać jednocześnie autoryzację dostępu do aplikacji WWW, aplikacji J2EE, oraz nawet do innych niewebowych aplikacji (aplikacje z klientem, na platformę MS Windows lub Linux)

Czym jest Access Manager

Rozwiązanie Access Manager dostarcza bezpieczny dostęp do zasobów i aplikacji umożliwiając sprawdzenie tożsamości użytkownika poprzez (ID, hasło, smartcard, token) i na tej bazie:

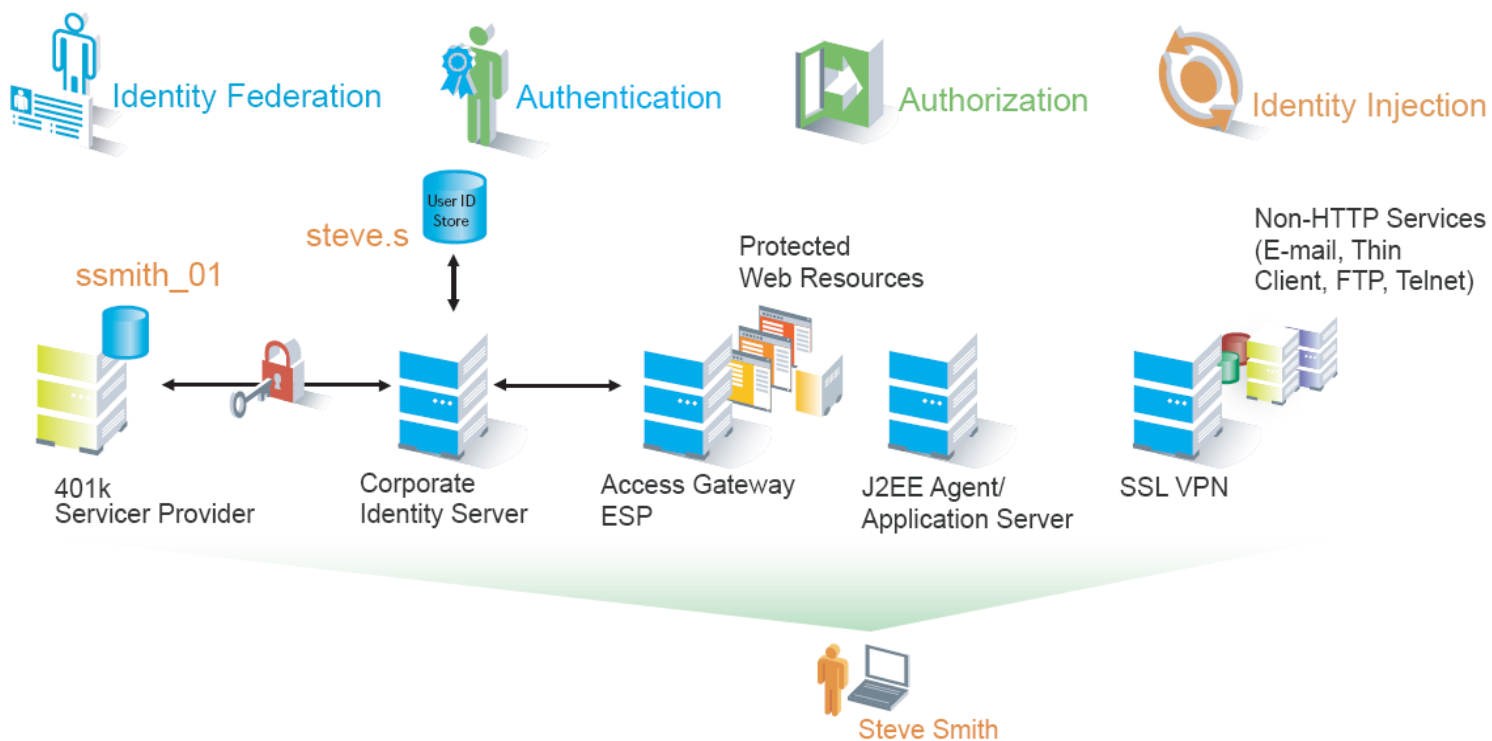
- Kontrolę dostępu oparta o role do zasobów WWW i aplikacji Webowych oraz pozostałych nie webowych aplikacji
- Single Sign-On dla aplikacji webowych, J2EE
- Szyfrowanie transmisji (SSL)
- Prezentacja informacji o zidentyfikowanym użytkowniku do aplikacji umożliwiającą dalszą personalizację obsługi
- Obsługa Libery Alliance





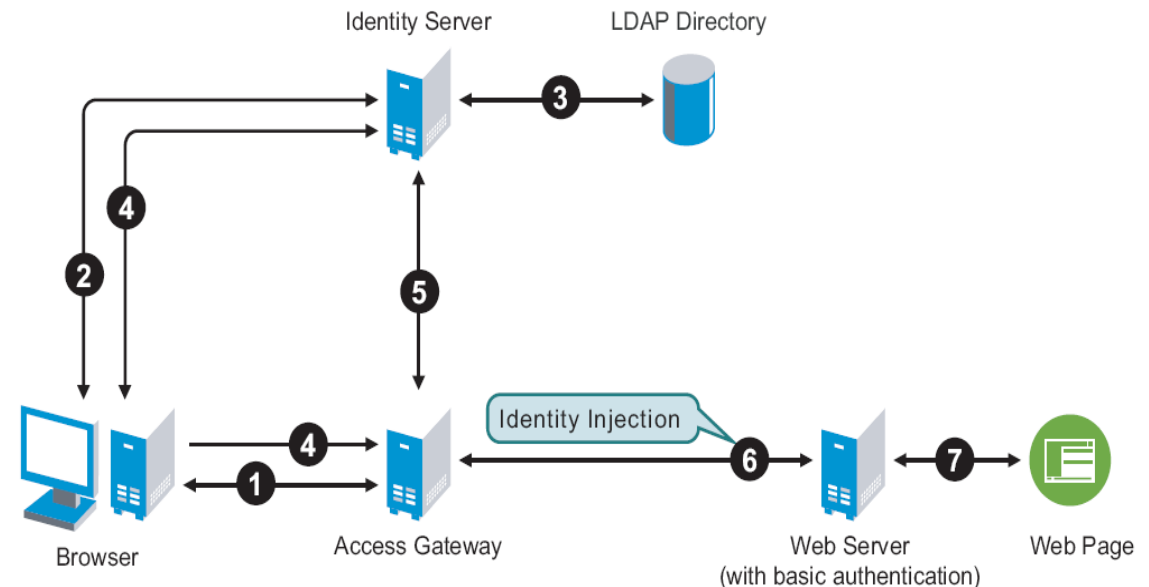
Novell Access Manager

Widok ogólny

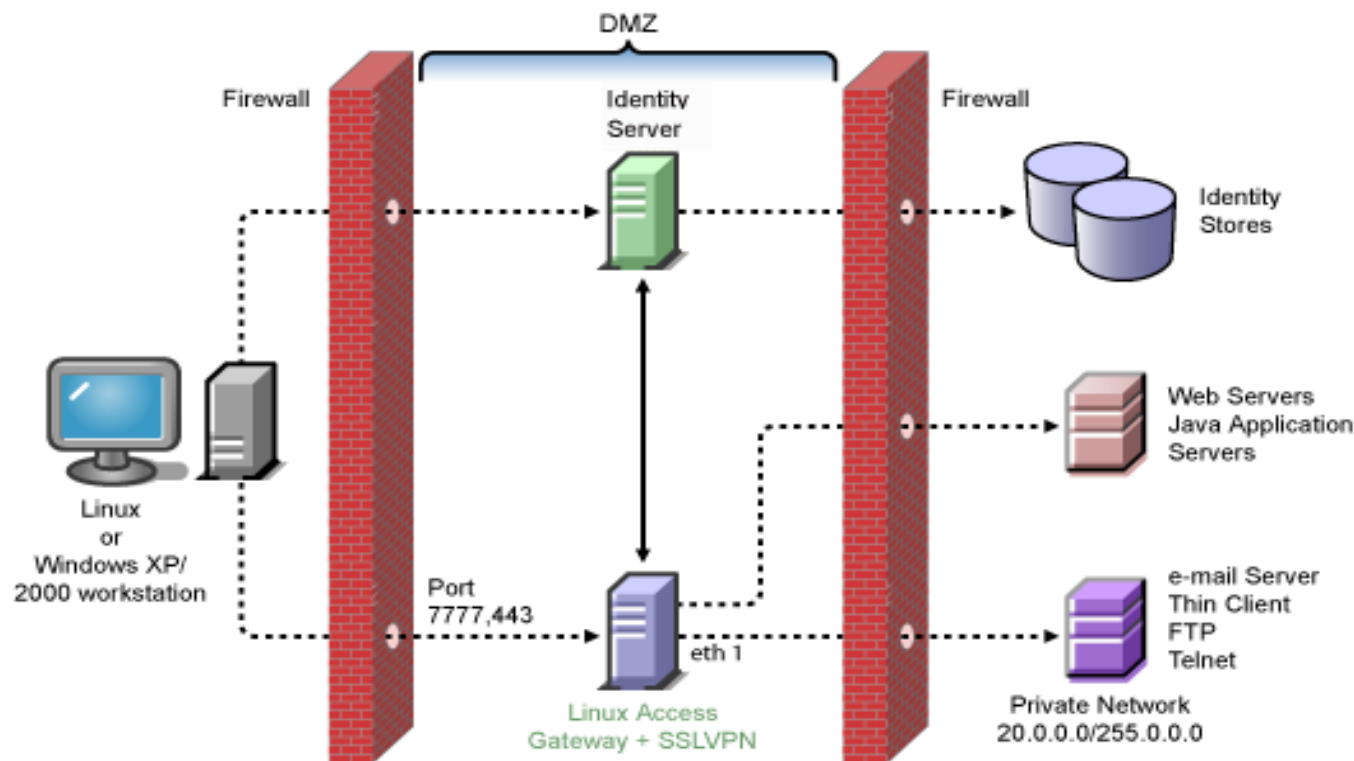


Zarządzanie dostępem do aplikacji webowych – Access Gateway

1. Użytkownik wybiera chroniony URL
2. Access Gateway przekierowuje do Identity Servera, który pyta o konto/hasło
3. Identity Server sprawdza w katalogu eDirectory, Active Directory, Sun ONE
4. Identity Server zwraca sukces do przeglądarki, która wraca do bramki Access Gateway
5. Access Gateway uważa użytkownika za uwierzytelnionego i pobiera informacje o nim
6. Access Gateway stosuje regułę „Identity Injection”, wstawia do nagłówka HTTP stosowne informacje i przesyła je do serwera www
7. Serwer www udostępnia dane



Zarządzanie dostępem do aplikacji niewebowych – SSL VPN



Użytkownik uwierzytelnia się raz przez dowolną przeglądarkę. Dostarczany jest w locie klient (ActiveX lub Java) do bezpiecznej komunikacji dla aplikacji niewebowych (SSL VPN).

Przed zestawieniem połączenia można wymusić sprawdzenie niezbędnego oprogramowania na stacji roboczej (osobisty firewall, antywirus)

Reguły Access Managera umożliwiają kontrolę, do jakich aplikacji można mieć dostęp

Access Manager – reguły

- Wykorzystanie informacji o roli użytkownika

Edit Policy: Deny_All_but_Manager - Rule 1 [?]

Type: Access Gateway: Authorization
Description: Deny All but Manager to Web Resource
Priority: 1

Conditions Condition structure: AND Conditions, OR group

If

Condition Group 1 [X] [↕]

New

If Not Roles for Current User [i] [X] [↕]

Comparison: String : Equals
Mode: Case Sensitive
Value: Roles Manager
Result on Condition Error: False

Append New Group

Actions

Do Deny Deny Message
You are not authorized to access this site.

Changes made on this panel must be applied from the [Policies](#) Panel.

OK **Cancel**

Access Manager – reguły

- Reguły złożone

Edit Policy: Auth_Policy_for_Sales_Dept ?

Type: Access Gateway: Authorization
 Description: Sales Department

Rule List

[New](#) | [Enable](#) | [Disable](#) | [Delete](#) 4 item(s)

<input type="checkbox"/>	Rule	Priority	Enabled	Action	Description
<input type="checkbox"/>	<u>1</u>	1	<input checked="" type="checkbox"/>	Permit	Sales Representative
<input type="checkbox"/>	<u>2</u>	2	<input checked="" type="checkbox"/>	Permit	Sales Manager
<input type="checkbox"/>	<u>3</u>	4	<input checked="" type="checkbox"/>	Permit	Sales President
<input type="checkbox"/>	<u>4</u>	10	<input checked="" type="checkbox"/>	Deny	Deny

Changes made on this panel must be applied from the [Policies](#) Panel.

OK | **Cancel**

Access Manager – reguły

- Reguły autoryzacyjne

Type: Access Gateway: Authorization

Description: Sales Department Permit Rule

Priority: 1

Conditions Condition structure: AND Conditions, OR group:

Condition Group 1

New

Roles for Current User

Comparison: String : Equals

Mode: Case Sensitive

Value: Roles : Manager

Result on Condition Error: False

And If

Liberty User Profile: Corporate Employment Identity:Department

Comparison: String : Equals

Mode: Case Insensitive

Value: Data Entry Field : Sales

Result on Condition Error: False

Actions

Do Permit

Access Manager – reguły

- Reguły autoryzacyjne („od czapy”)

Type: J2EE Agent: Web Authorization

Description:

Priority:

Conditions Condition structure: AND Conditions, OR groups

If

Condition Group 1

New

If LDAP Attribute: hatSize
 Comparison: Integer : Equals
 Value: Data Entry Field : 10
 Result on Condition Error: True

Append New Group

Actions

Do Deny

Changes made on this panel must be applied from the [Policies](#) Panel.

OK Cancel

Access Manager – reguły

- Wstawianie informacji o tożsamości („Identity Injection”)

Type: Access Gateway: Identity Injection

Description:

Priority: 1

Actions

New

Do Inject into Authentication Header

User Name: Authentication Contract

Password: Authentication Contract

Multi-Value Separator: ,

DN Format: LDAP (ex, cn=jsmith,ou=Sales,o=Novell)

Actions

New

New

- Inject into Authentication Header
- Inject into Custom Header
- Inject into Custom Header with Tags
- Inject into Cookie Header
- Inject into Query String

Ch: Policies Panel.

Actions

New

Do Inject into Custom Header with Tags

Custom Header Name:

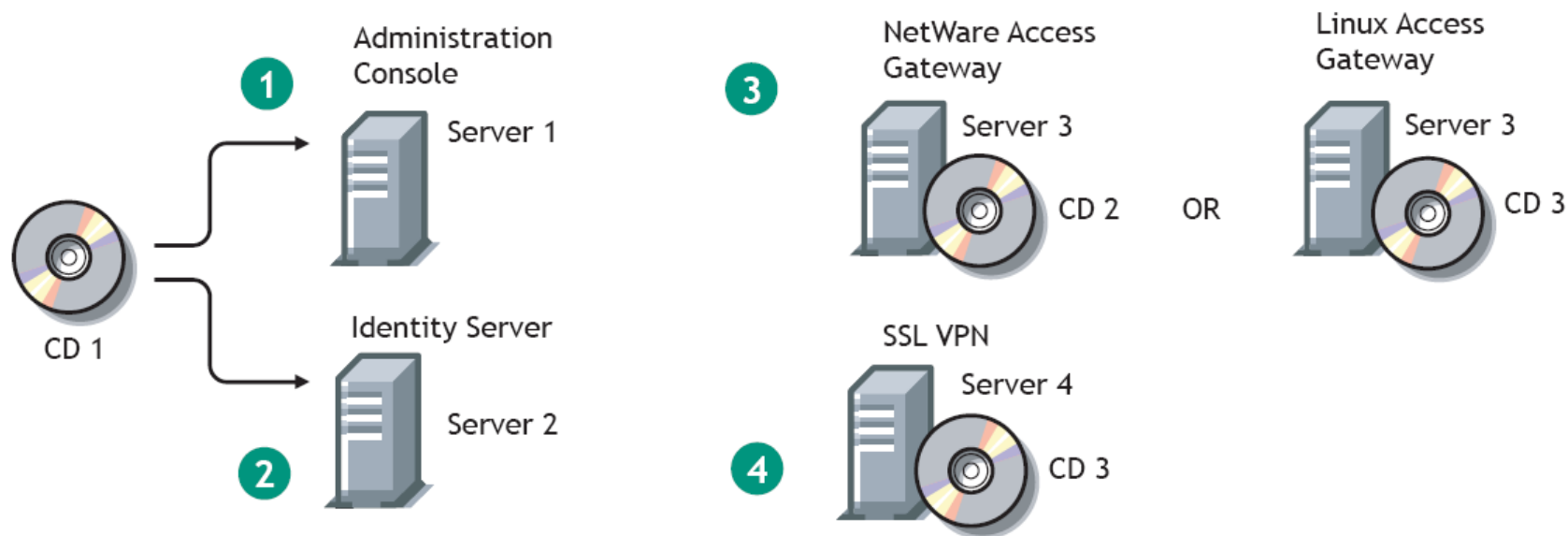
Tags

Tag Name	Tag Value
<input type="text"/>	Authentication Contract <input type="button" value="v"/>

Multi-Value Separator: ,

DN Format: LDAP (ex, cn=jsmith,ou=Sales,o=Novell)

Instalacja i wymagania dla poszczególnych elementów



Wymagania: OGÓLNE

- Serwer z katalogiem LDAP (eDirectory 8.7 lub późniejszy, Sun ONE bądź Active Directory)
- Serwery WWW, których zawartość ma podlegać ochronie
- Klient z przeglądarką: Internet Explorer co najmniej 6 SP1 bądź Mozilla Firefox co najmniej 1.5 (odblokowane dynamiczne okienka)
- Przełącznik L4, jeśli planowany jest rozkład obciążenia (*hardware/software*)
- Stałe adresy IP
- Serwer DNS
- Synchronizacja czasu (różnica \leq 1 min.)

Wymagania: konsola administracyjna

- Windows Administration Console:
 - Windows Server 2003 or Windows 2008 R2 Enterprise Server
- Linux Administration Console:
 - SLES 10 SP2 i nowszy, SLES 11, SLES 11 SP1
- 4 GB RAM (minimum).
- 100 GB dysk (30 GB minimum) ze względu na kronikę
- Brak OpenLDAP, iManagera i eDirectory
- Pakiety: gettext, python, compat

Wymagania: Identity Server

- 100 GB dysk (30 GB minimum), 4 GB RAM
- Procesor Dual CPU lub Core (co najmniej 3.0 GHz)
- Windows Identity Server:
 - Windows Server 2003 lub Windows 2008 R2 Enterprise Server
- Linux Identity Server:
 - SLES 10 SP2 i nowszy, SLES 11 lub SLES 11 SP1.
 - Gettext, python (interpreter), compat
- Statyczny adres IP
- Brak OpenLDAP, który domyślnie jest instalowany

Wymagania: Access Gateway

- Dysk 100 GB
- 4 GB RAM
- Procesor Dual CPU lub Core (3.0 GHz)
- Statyczny adres IP
- Brak wymogów dot. oprogramowania
 - Program instalacyjny zawiera Access Gateway Appliance, który tworzy nowy obraz dysku i zawiera już system SLES 11

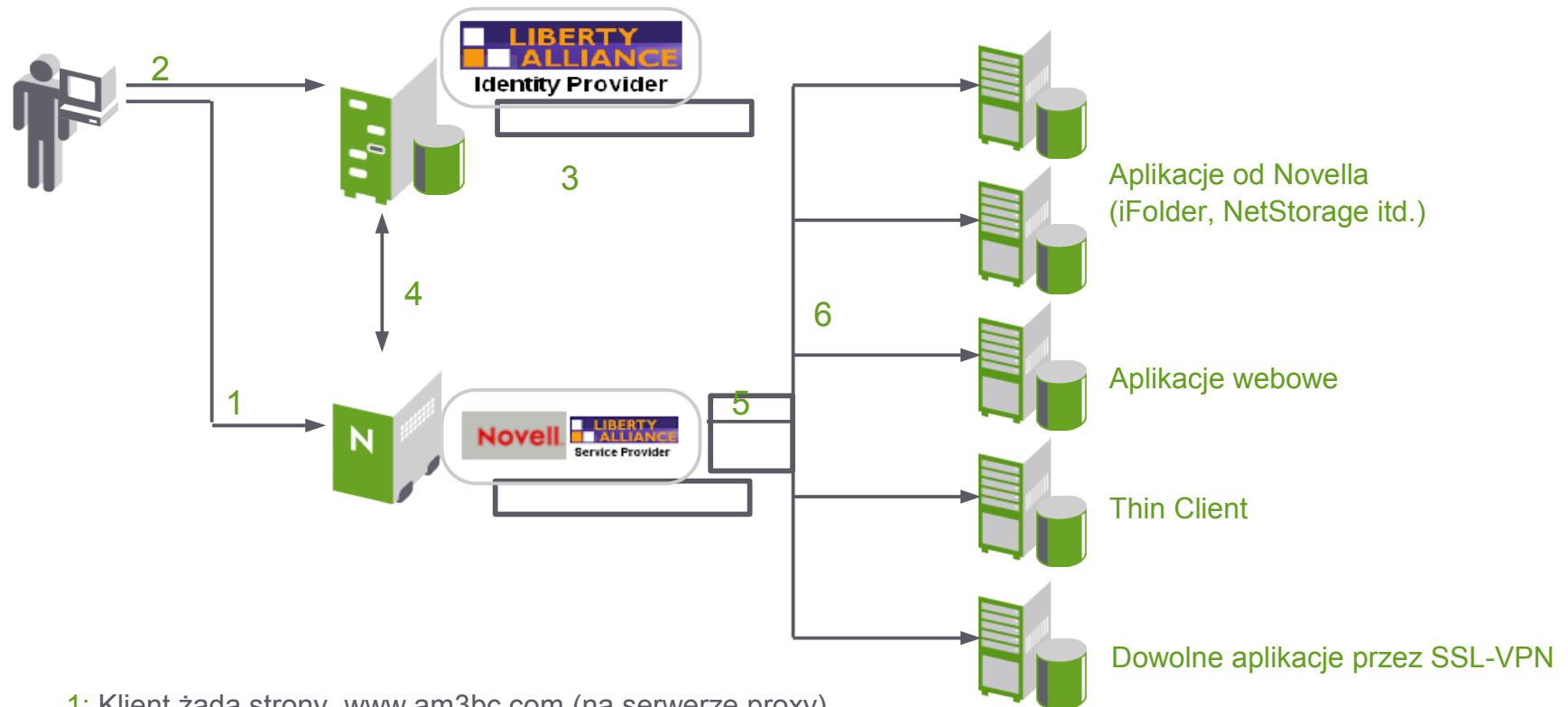
Wymagania: SSL VPN klient

- Windows 2000SP4 / XPSP2 / Vista / 7 32- i 64-bit.
 - Internet Explorer od wersji 6.0 (SP2)
 - Mozilla Firefox od wersji 2.x
- Linux
 - SUSE Linux Enterprise Desktop 10 i 11, 32- lub 64-bit
 - Firefox od wersji 2.0
 - JRE 1.5.0_11 lub nowsza, OpenSSL 0.9.7, Shells: bash i xterm
- Macintosh:
 - Mac PPC 10.4 Tiger, Mac Intel 10.5 Leopard, Mac OSX 10.6 Snow Leopard
 - Mac Safari od wersji 2.0.4 build 412, Firefox od 2.0
 - JRE 1.5.0_11 lub nowsza, OpenSSL 0.9.7, bash shell

Wymagania: SSL VPN Server

- Dysk 100 MB, 4 GB RAM
- Co najmniej dwie karty sieciowe
- Procesor Dual CPU lub Core (3.0 GHz)
- System SLES 10 SP1, SP2 lub SP3, 32-bit lub 64-bit.
SLES 11, 32-bit lub 64-bit
 - gettext, Tomcat & Java
- Port TCP 7777

Access Manager – obsługa Liberty Alliance



- 1: Klient żąda strony www.am3bc.com (na serwerze proxy)
- 2: Następuje przekierowanie w celu uwierzytelnienia (poprzez dostawcę tożsamości Identity Provider)
- 3: Identity Provider uwierzytelnia i określa rolę użytkownika
- 4: Ponowne przekierowanie. Tym razem do serwera proxy
- 5: Dostęp udzielony (lub nie)
- 6: Dodatkowe informacje o użytkowniku przekazane aplikacji www

Licencjonowanie i ceny

Access Manager – licencjonowanie

Na użytkownika, dla którego wymagamy uwierzytelniania

- Novell Access Manager 3.1 1-User License + 1-Year Standard Maintenance za 15 euro
- 2,9 euro za użytkowników nieaktywnych (logowanie co 120 i więcej dni)

Serwery bez dodatkowych opłat

Specjalna, 10 razy tańsza licencja dla projektów, gdzie użytkownikami są klienci firmy lub klienci urzędu:

- Novell Access Manager 3.1 1-User Government-to-Citizen/Business-to-Consumer/Business-to-Consumer License + 1-Year Standard Maintenance



Novell Access Manager w Twojej organizacji

- Mamy specjalne ceny dla różnych grup odbiorców (np. administracja, edukacja, szpitale)
- Skorzystaj z indywidualnej wyceny i formularza zamówienia oferty:
 - www.novell.pl/formularz.html
- Więcej informacji o produkcie
 - www.novell.com/products/accessmanager
 - infolinia 800 22 66 85

Unpublished Work of Novell, Inc. All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. Novell, Inc. makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. Further, Novell, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

