

HI MY NAME IS ANTHONY VAN DEN BOSSCHE, TECHNICAL CONSULTANT

# How to secure Hybrid Identities

What are the problems we are facing today?

What are present opportunities?

Application Publishing

DEMO!



**REALDOLMEN**  
to get there, together

# Problems of the past/present

- Loads of **overpowered accounts**
- No or very limited **audit trail**
- **Applications** are getting **published**
  - ▶ However, not always in a secure manner
  - ▶ Complex application architecture
  - ▶ Difficult seeing the forest from the trees
- No proper **User Lifecycle Management**
- **Multifactor** authentication is not leveraged
- No strong **password policies** exist
- Logon behaviour is not monitored
- Multiple sets of credentials



# Opportunities of the present/future

- Use Azure AD as an Identity Provider
- Extend identities towards the Cloud
- Application delivery using Azure AD App Proxy
- Machine learning on logon behaviour
- Just-in-time access and rbac
- Conditional Access Policies
- Leverage an ever-evolving platform
- Easy MFA integration



# Application Publishing

Seeing the forest from the trees



**REALDOLMEN**  
to get there, together

# Publishing Applications the old way

- Punch holes through firewalls (edge and perimeter)
- Leverage expensive Hardware Load Balancers
  - F5 BigIP, Kemp, Netscaler
- Costly setup and operational management
- Far reaching knowledge required
- Domain Controllers in DMZ! (RODC best case)
- High TCO (Compute, Networking, Storage)
  - Cooling, electricity, hardware failures



# Azure Active Directory

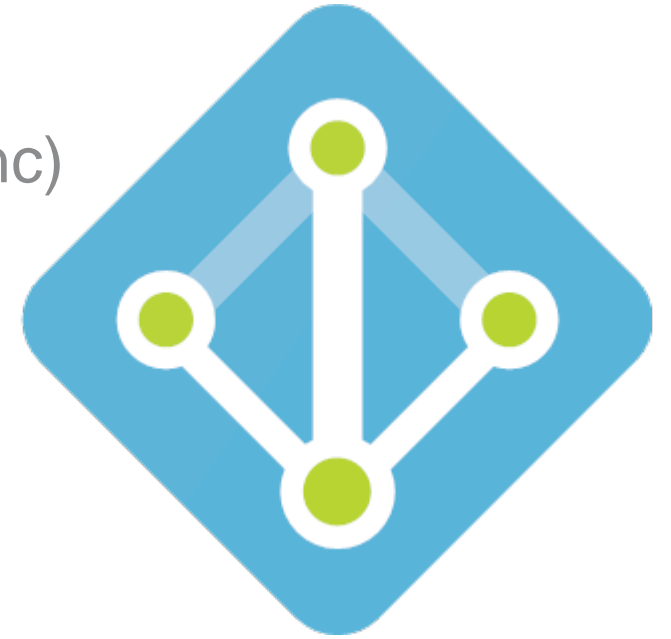
Extending Identities towards the Cloud



**REALDOLMEN**  
to get there, together

# Azure Active Directory

- Identity Bridge thanks to ADConnect (AADSync-DirSync)
- Identity Provider – Security Token Service
- Outside-perimeter protocols
  - ▶ ~~Windows Authentication: Kerberos, NTLM~~
  - ▶ SAML, WSFederation
  - ▶ OpenID Connect, Oauth2 (Modern Authentication)
- Administration through PoSh, REST Api, Azure Portal(s)
- Numerous Cloud-driven (cloud-born) features
  - ▶ App Proxy, Self Service, PIM, Identity Protection, Collaboration



# Azure AD Application Proxy

Publishing apps with least amount of effort/cost



**REALDOLMEN**  
to get there, together






# Azure AD App Proxy


- No on-premises hardware needed! DMZ still needed?
- No more “Firewall hole punching”! Only outbound traffic!
  - Recently publically available: **only port 80 and 443**
- Co-op with Azure AD Security Token Service
  - Federation Conditional Access, Multifactor Authentication
- Profit from machine learning on the Azure AD platform
  - PIM, Identity Protection
- Incredibly easy to publish applications
  - Claims Aware, Windows Authentication, Anonymous, Forms Based
- Auto-updating connectors so no more firmware upgrades
- Secure endpoints (SSL Labs)
- Instant collaboration

# High Level install/config steps – Enable feature


- Logon to your tenant
- Enable Azure AD App Proxy on your tenant

---

 New connector group    Download connector    Enable application proxy

 Application proxy is currently disabled for your tenant

- Default connector group already exists

CONNECTOR	IP	STATUS
 ▶ Default		

# High Level install/config steps – Install connectors

- Download connector from Azure Portal
- Install proxy on selected machines



## Azure AD Application Proxy Connector Download

Download and install the Application Proxy connector to enable a secure connection between applications inside your network and the Application Proxy. Only one installation is necessary to service all your published applications; a second connector can be installed for high availability purposes.

### System Requirements

- Operating systems:
  - Windows Server 2012 R2
  - Windows Server 2016
- Make sure the connector's communication with the Application Proxy is not blocked by a firewall. To check that all required ports are open, please try our [port check tool](#).
- The connector must have access to all on premises applications that you intend to publish

### Installation Instructions

To install the Application Proxy connector, download the connector installation package and install it on a local, designated machine.

### Related Resources

For more information on the Application Proxy connector, see [our online content](#).


[I accept the license terms and privacy agreement](#)

**Download** (64 bit version)

# High Level install/config steps – Add application


- Add your application
- Select on-prem app
- Name the App
- Internal URL
- Authentication Type

Add your own app




Application you're developing

Register an app you're working on to integrate it with Azure AD



On-premises application

Configure Azure AD Application Proxy to enable secure remote access





Non-gallery application

Integrate any other application that you don't find in the gallery


## Add your own on-premises application

+ Add ✕ Discard

 Application Proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. Click here to learn more about Application Proxy. 

\* Name ⓘ  ✓

\* Internal Url ⓘ  ✓

External Url ⓘ   ✓   

Pre Authentication ⓘ  ▼

Translate URL in Headers? ⓘ

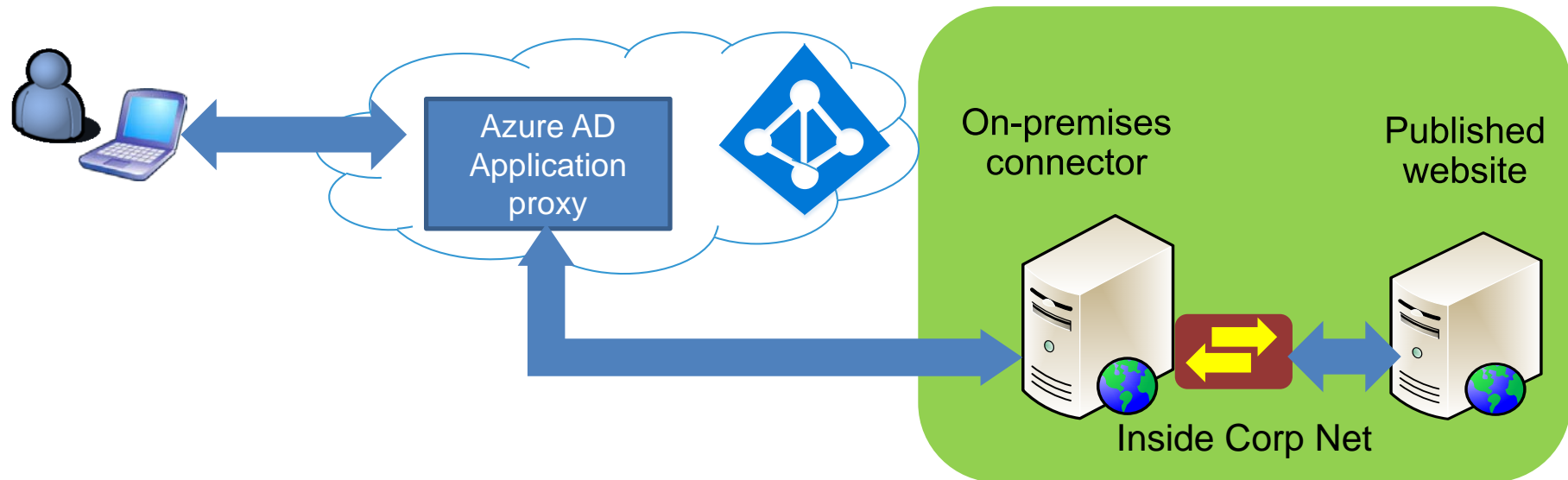
Backend Application Timeout ⓘ  ▼

Connector Group ⓘ  ▼

# Azure AD Application Proxy

## High Level Overview

- Connectors on-prem have a communication channel with proxy (**outbound**)
- Use Microsoft domainname **tenantname.msapproxy.net**
- **Or** use your own domain name and create CNAME



# Azure AD App Proxy licensing info

- Not available in “free” edition (Office 365 only tenant)
- Available for **Basic** and **Premium (P1–P2)** licences
- **Basic**

	ENTERPRISE AGREEMENT	ONLINE
Prijs	Neem contact op met uw vertegenwoordiger van <a href="#">Enterprise Overeenkomst</a>	€0,844 gebruiker / maand*

- **Premium P1 (Self Service, MFA, MIM)**

	ENTERPRISE AGREEMENT	ONLINE
Prijs	Neem contact op met uw vertegenwoordiger van <a href="#">Enterprise Overeenkomst</a>	€5,06 gebruiker / maand*

- **Premium P2 (Identity Protection, PIM)**

	ENTERPRISE AGREEMENT	ONLINE
Prijs	Neem contact op met uw vertegenwoordiger van <a href="#">Enterprise Overeenkomst</a>	€7,59 gebruiker / maand*

# Azure AD Application Proxy Demo

Setup, pass-through, pre-authentication, MFA, Identity Protection



**REALDOLMEN**  
to get there, together

# Q&A



**REALDOLMEN**  
to get there, together







To get there, together



**REALDOLMEN**



**HQ Realdolmen Huizingen**

A. Vaucampsiaan 42

B-1654 Huizingen

+32 2 801 55 55

[www.realdolmen.com](http://www.realdolmen.com)