Virtual Identity Server™

The .NET Virtual Directory™
### LDAP Proxy Firewall Server

Many organizations utilize an http web proxy server, such as Microsoft's Internet Security and Acceleration (ISA) Server within their web server environment. ISA provides not only a more secure environment, but also additional performance capabilities.

*Likewise, the **Virtual Identity Server™ (VIS™)**, deployed as an LDAP proxy firewall server offers this type of protection and security for LDAP directories such as Active Directory. Applications connect to the VIS proxy server exactly as they do any normal LDAP directory. In fact, VIS looks and behaves just like a standard Active Directory or ADAM server to the LDAP enabled client application.*

ISA - HTTP Web Proxy Server
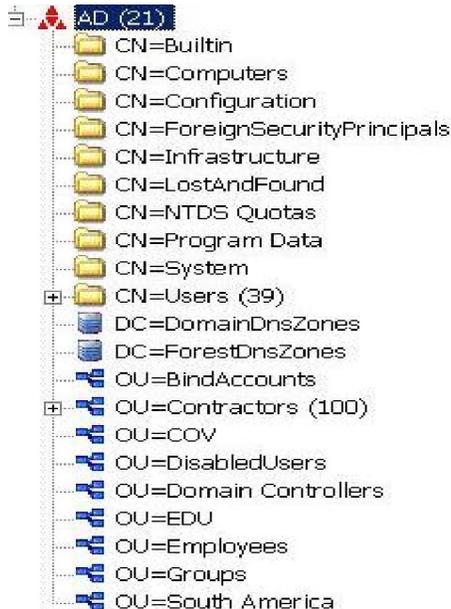

VIS - LDAP Proxy Server
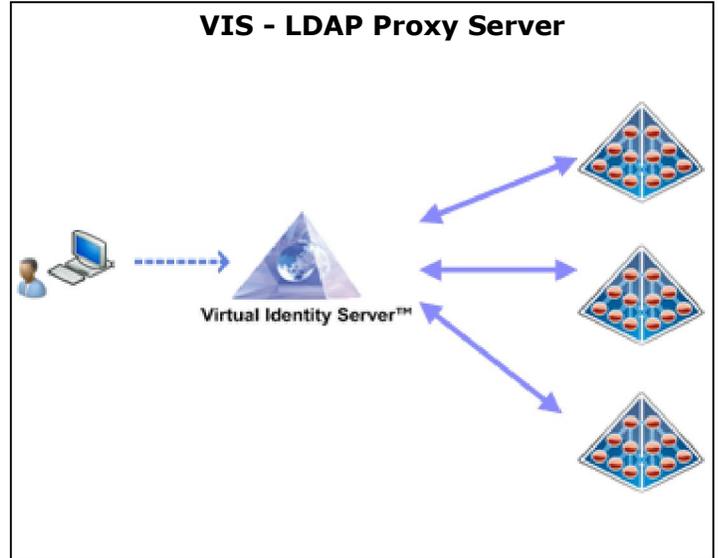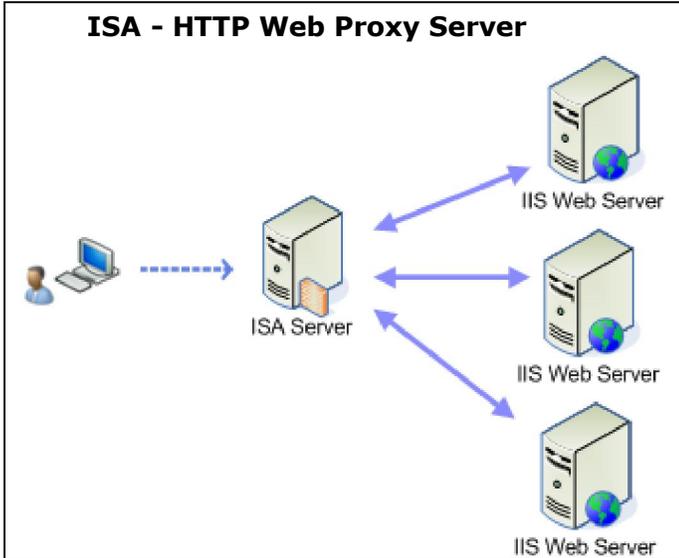
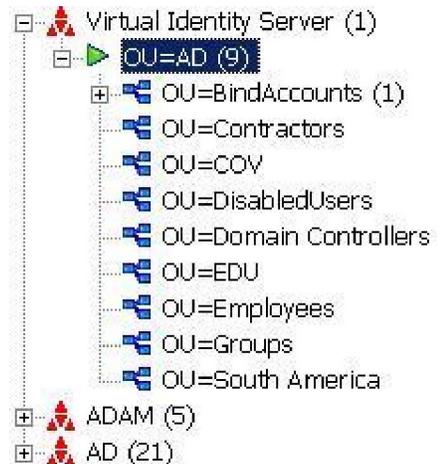### The Virtual Identity Server provides application specific views

In many cases, applications that are written to Active Directory are written poorly and inefficiently. For example, many applications connect at the root of the Active Directory forest when they may only need to search one or two containers in the tree. Additionally, many applications only need to view users and groups, but in reality are granted access to view more than just users and groups.

VIS easily maps and publish application specific views, granting only the data the application requires.

Normal AD View

- AD (21)
  - CN=Builtin
  - CN=Computers
  - CN=Configuration
  - CN=ForeignSecurityPrincipals
  - CN=Infrastructure
  - CN=LostAndFound
  - CN=NTDS Quotas
  - CN=Program Data
  - CN=System
  - CN=Users (39)
  - DC=DomainDnsZones
  - DC=ForestDnsZones
  - OU=BindAccounts
  - OU=Contractors (100)
  - OU=COV
  - OU=DisabledUsers
  - OU=Domain Controllers
  - OU=EDU
  - OU=Employees
  - OU=Groups
  - OU=South America

VIS - Filtered View

- Virtual Identity Server (1)
  - OU=AD (9)
    - OU=BindAccounts (1)
    - OU=Contractors
    - OU=COV
    - OU=DisabledUsers
    - OU=Domain Controllers
    - OU=EDU
    - OU=Employees
    - OU=Groups
    - OU=South America
  - ADAM (5)
  - AD (21)

Active Directory Only

- **Active Directory is vulnerable and unsecure** to attacks such as denial of service.

- **Applications have more access then they need** with the principle of least privilege being very hard to enforce.

- **Data in Active Directory is difficult to secure** because administrators have little control over the applications accessing the data.

- **Poorly written application can crash AD** causing outages for end users.

- **Active Directory performance is susceptible** to inefficient queries that applications send.

Technical Specifications

Windows Server 2003 or Windows Server 2008
.NET 4.0 Framework or greater
Runs as standard Windows service
Built-in Audit Logging (Requires SQL Server)

Adapters:
Active Directory (AD)
Active Directory Application Mode (ADAM)
Active Directory Lightweight Directory Services (AD LDS)
Novell eDirectory
Sun One Directory Server (iPlanet)
Oracle Internet Directory (OID)
Tivoli Directory Server
OpenLDAP
Generic LDAP V3 Server
Microsoft SQL Server Database
Oracle Database
Google Cloud
Custom sources such as: RACF, AS/400 via Extensibility

Active Directory with VIS

- **Active Directory is more secure** by being placed behind an LDAP firewall proxy server. Applications no longer access AD directly.

- **VIS provides data leakage prevention (DLP)** by only publishing the data that the applications require.

- **Active Directory is now protected and safe** because inefficient or rogue queries are either blocked or transformed in real-time into more efficient queries.

- **VIS provides a complete auditing solution** for all applications accessing AD. All activity (modifications, searches) are captured.

- **Administrators can profile applications** seeing exactly what the applications are searching and modifying in the directory.

- **All applications have built-in failover** as backend systems fail, VIS provides the failover mechanisms automatically at the server layer.

- **All applications have built-in connection pooling** to AD, which increases performance and reliability significantly.

- **Application deployment time is reduced by over 50%** by quickly providing real-time application specific views from multiple data stores.

- **VIS removes application deployment barriers** by handling AD schema changes virtually and rapidly providing multi-forest views without any forest trusts.

- **VIS reduces the Kerberos token size limit** problem by providing application specific groups at the VIS layer.

- **Active Directory and application performance is increased** by filtering data.

About Optimal IdM, LLC.

Optimal IdM, LLC. is a leading global provider of identity management software and consulting solutions. Headquartered in Land O' Lakes, Florida, Optimal IdM provides sales and services through regional offices across the United States and a growing network of resellers and distributors.

Optimal IdM's customers include Fortune 1000 companies, as well as, Federal, State and Local Government agencies in more than 12 countries on 4 continents. Founded in 2005, Optimal IdM is privately held and has been profitable in every quarter since inception.

For more information on our products and services, please visit our website at http://www.optimalidm.com or call +1.813.425.6351

Optimal IdM, LLC.
2209 Collier Parkway, Suite 140
Land O' Lakes, FL 34639
Email: Sales@optimalidm.com
Phone +1.813.425.6351
Fax   +1.813.425.6351