Vordel Gateway Deployment White Paper

Vordel Gateway 6

Appliance and Software

Contacting Vordel

Vordel is dedicated to producing appliances and software of excellent quality and welcomes feedback on any Vordel products. For more information about Vordel, and its advanced suite of SOA appliances and software, visit the Vordel web site: www.vordel.com.

If you encounter an issue, please contact Vordel, and provide the following information:

- Description of the issue
- Any relevant messages provided by the system
- Diagnostic output (for example, trace files)
- Configuration information from the /conf directory
- Appliance / software version and platform

Customer support: support@vordel.com
Sales enquiry: sales@vordel.com
Website: www.vordel.com
Customer extranet: extranet.vordel.com

Note: All examples in this document refer to the Vordel Gateway version 6.x. Therefore, it may contain references to features not included in earlier versions.

Last updated: 1/16/2012

Table of Contents

1 Introduction

This document answers the typical questions that customers ask when deploying Vordel 6.x Gateways. Enterprises use the software and appliance versions of these products to perform a broad range of XML processing scenarios and tasks, including, but not limited to the following:

- Security
- Application offload
- Service level enforcement
- Service virtualization
- Protocol mediation for XML traffic

2 Architecture

Businesses today are exploiting XML and Web Services to enable rapid application integration internally across the enterprise and externally with trading partners, suppliers and end-customers. Regardless of what stage an enterprise is along the path of XML adoption, be it for tactical point-to-point XML-based integration projects through to the full-blown roll out of Services Oriented Architecture (SOA), Vordel's solution addresses the requirements of this wave of integration.

Vordel 6 is a set of enterprise XML network infrastructure products that addresses the key requirements of XML-based integration and SOA. The following diagrams show the logical and physical architecture of Vordel 6:

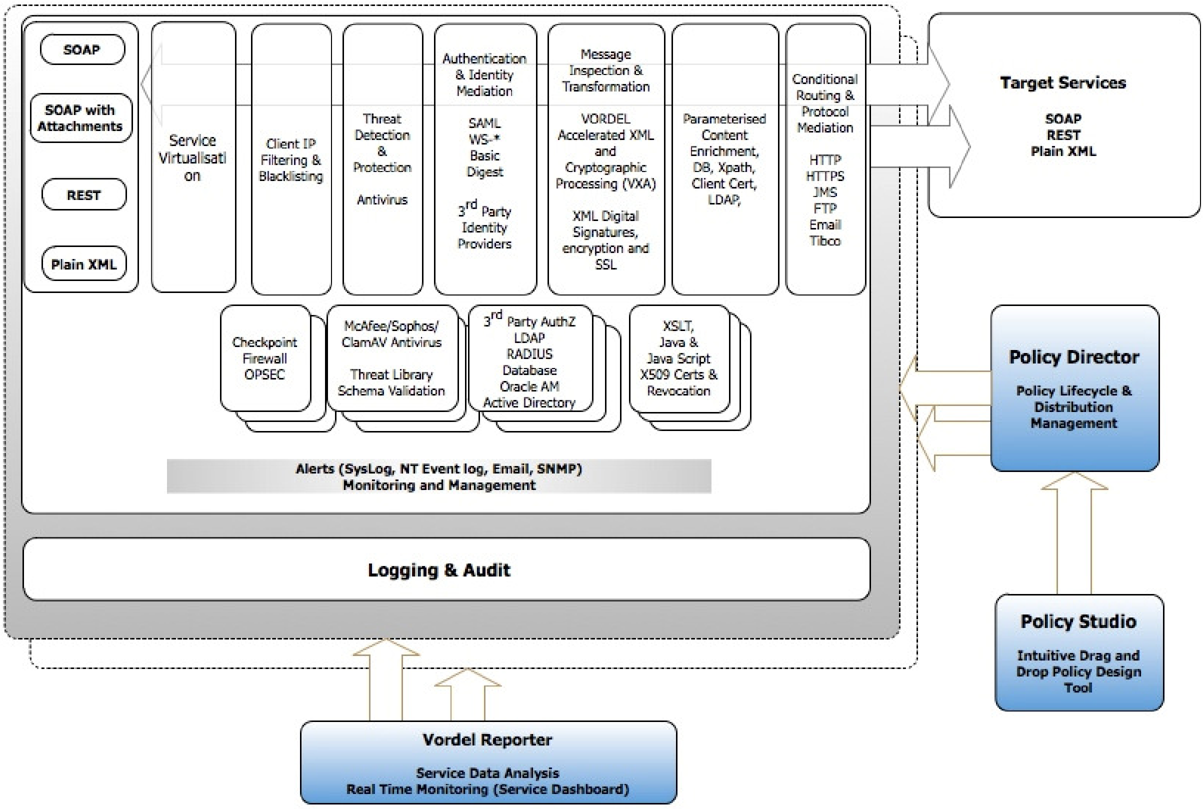

SOAP
SOAP with Attachments
REST
Plain XML
Service Virtualisati on
Client IP Filtering & Blacklisting
Threat Detection & Protection
Antivirus
Authentication & Identity Mediation
SAML
WS-*
Basic
Digest
3rd Party Identity Providers
Message Inspection & Transformation
VORDEL Accelerated XML and Cryptographic Processing (VXA)
XML Digital Signatures, encryption and SSL
Parameterised Content Enrichment, DB, Xpath, Client Cert, LDAP,
Conditional Routing & Protocol Mediation
HTTP
HTTPS
JMS
FTP
Email
Tibco
Checkpoint Firewall OPSEC
McAfee/Sophos/ ClamAV Antivirus
Threat Library Schema Validation
3rd Party AuthZ
LDAP
RADIUS
Database
Oracle AM
Active Directory
XSLT, Java & Java Script
X509 Certs & Revocation
Alerts (SysLog, NT Event log, Email, SNMP)
Monitoring and Management
Logging & Audit
Target Services
SOAP
REST
Plain XML
Policy Director
Policy Lifecycle & Distribution Management
Policy Studio
Intuitive Drag and Drop Policy Design Tool
Vordel Reporter
Service Data Analysis
Real Time Monitoring (Service Dashboard)

Figure 1: Logical Architecture

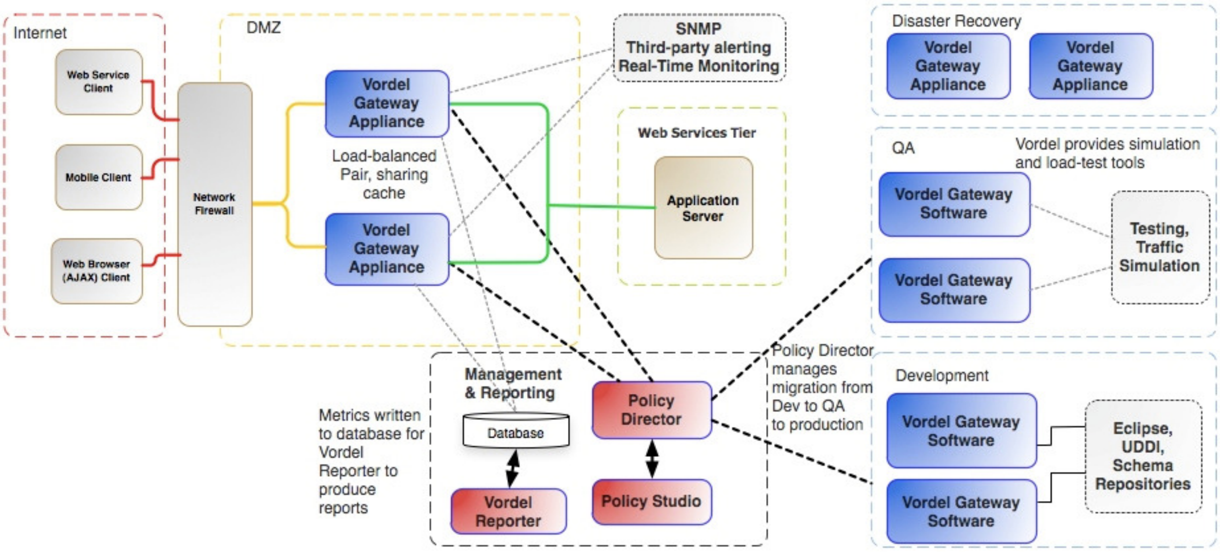


Figure 2: Physical Architecture

3 Form Factors

Vordel is available in software and hardware forms:

- Appliance (hardware / software combination): includes a crypto acceleration card and optionally a Hardware Security Module (HSM)
- Virtual Appliance (virtual image of the appliance): for VMware, Oracle VM, and Amazon EC2
- Software: installable for Windows, Linux, and Solaris Sparc

Typically, Vordel customers use a mix of software for development and initial testing of policies, with appliances used for preproduction and production systems.

4 Advantages of Choosing an Appliance

The advantages of choosing an appliance over software are:

- Performance is significantly enhanced by the inclusion of a cryptographic acceleration card
- The appliance platform is pre-hardened and has been through extensive security testing
- The complete solution is available in a single package simplifying support and purchasing
- Vordel's powerful Web Administration Interface is included in the appliance platform
- Logging, monitoring, and network configuration are pre-integrated in the appliance platform
- All of the components have gone through an extensive QA and are certified to work well together

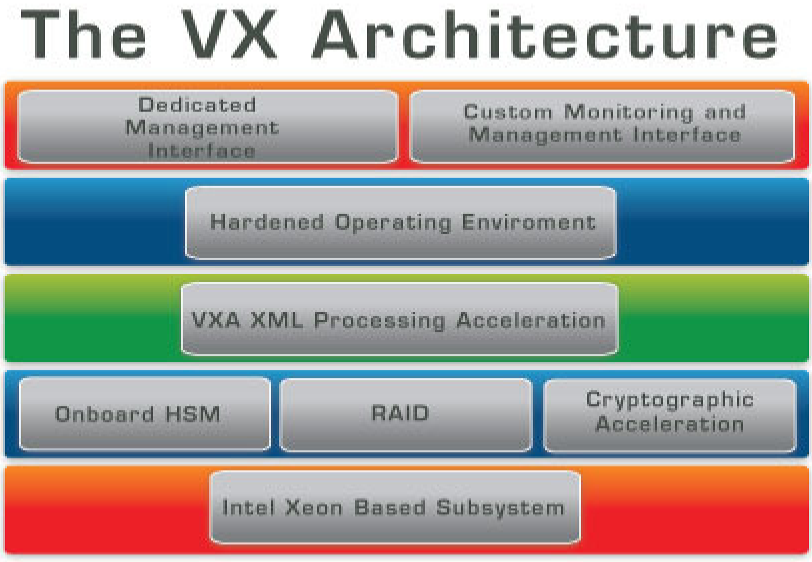

The VX Architecture
Dedicated Management Interface
Custom Monitoring and Management Interface
Hardened Operating Enviroment
VXA XML Processing Acceleration
Onboard HSM
RAID
Cryptographic Acceleration
Intel Xeon Based Subsystem

Figure 3: VX Architecture

5 Who Owns the XML Networking Infrastructure?

Vordel products are administered by two distinct groups:

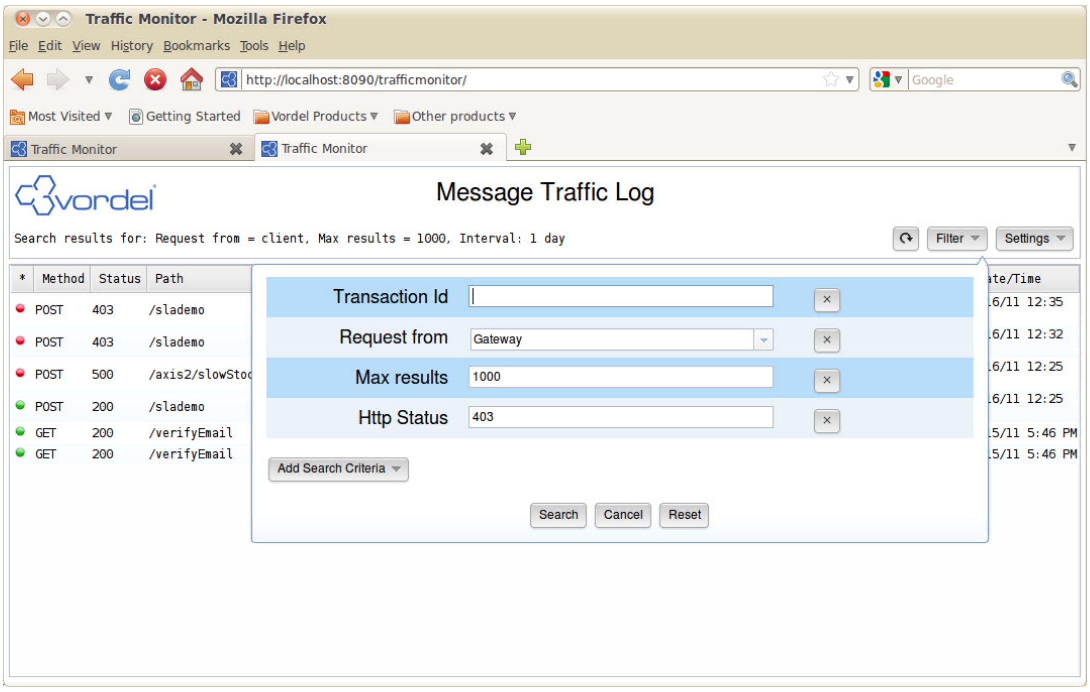
- Operations: the runtime management of XML data traffic, logs and alerts, and high-availability is performed by Operations staff.
- Architecture (Security Architects and Systems Architects): the design-time policy definition, which defines the behavior of the XML networking infrastructure, is performed by architects.

5.1 Operations Staff

Operations staff are responsible for making sure that the Vordel Gateway is running correctly. They are concerned with the following problems:

- System status and health
- Network connectivity
- Security alerts
- System security
- Backups and recovery
- Maintenance of logs

The Vordel platform comes with an interface dedicated to the Operations team, called Traffic Monitor. The traffic monitor console helps quickly isolate failed or blocked transactions and provides a wealth of information about the transaction execution, payload, and so on.



Message Traffic Log

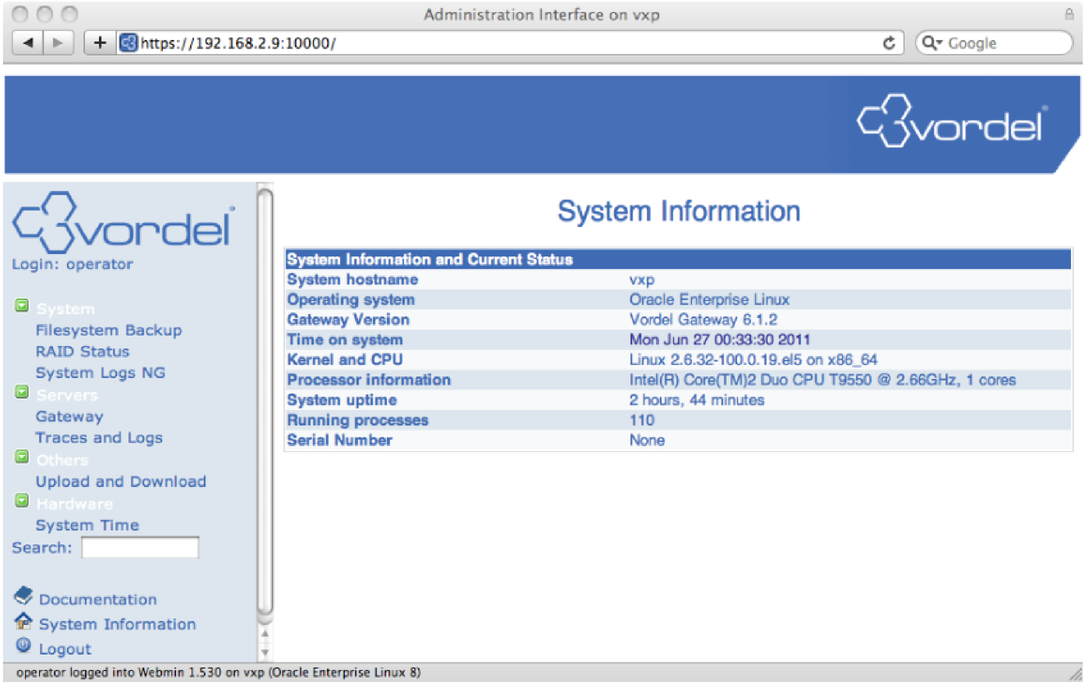
```
Search results for: Request from = client, Max results = 1000, Interval: 1 day
```

*	Method	Status	Path	te/Time
●	POST	403	/slademo	6/11 12:35
●	POST	403	/slademo	6/11 12:32
●	POST	500	/axis2/slowStoc	6/11 12:25
●	POST	200	/slademo	6/11 12:25
●	GET	200	/verifyEmail	5/11 5:46 PM
●	GET	200	/verifyEmail	5/11 5:46 PM

Transaction Id	
Request from	Gateway
Max results	1000
Http Status	403

Figure 4: Traffic Monitor Console

The appliance and virtual appliance platforms incorporate a powerful Web Administration Interface to control the common system specific tasks that are required by operations staff. The Web interface runs by default and makes the configuration of all system related tasks relatively quick and easy.



System Information

System Information and Current Status	
System hostname	vxp
Operating system	Oracle Enterprise Linux
Gateway Version	Vordel Gateway 6.1.2
Time on system	Mon Jun 27 00:33:30 2011
Kernel and CPU	Linux 2.6.32-100.0.19.el5 on x86_64
Processor information	Intel(R) Core(TM)2 Duo CPU T9550 @ 2.66GHz, 1 cores
System uptime	2 hours, 44 minutes
Running processes	110
Serial Number	None

operator logged into Webmin 1.530 on vxp (Oracle Enterprise Linux 8)

Figure 5: Web Administration Interface for Appliance

As well as providing operational management functionality of its own, the Vordel Gateway also interoperates with network operations tools such as HP OpenView, BMC Control, and CA UniCenter.

5.2 System Architects

System architects have an overarching view of enterprise IT infrastructures, and consequently are more concerned with using the Gateway to help integrate existing enterprise systems together. They want to be able to enable Web Services (WS-*) standards and integrate with third-party systems. A rich policy development application called Policy Studio enables system architects to create and control XML processing policies. Policy Studio visually defines workflows, so that configuration is done at a systems architect level, without the requirement to write code.

6 Where do you Deploy a Gateway?

Gateways can be deployed in the DMZ or in the LAN depending on policy or requirements:

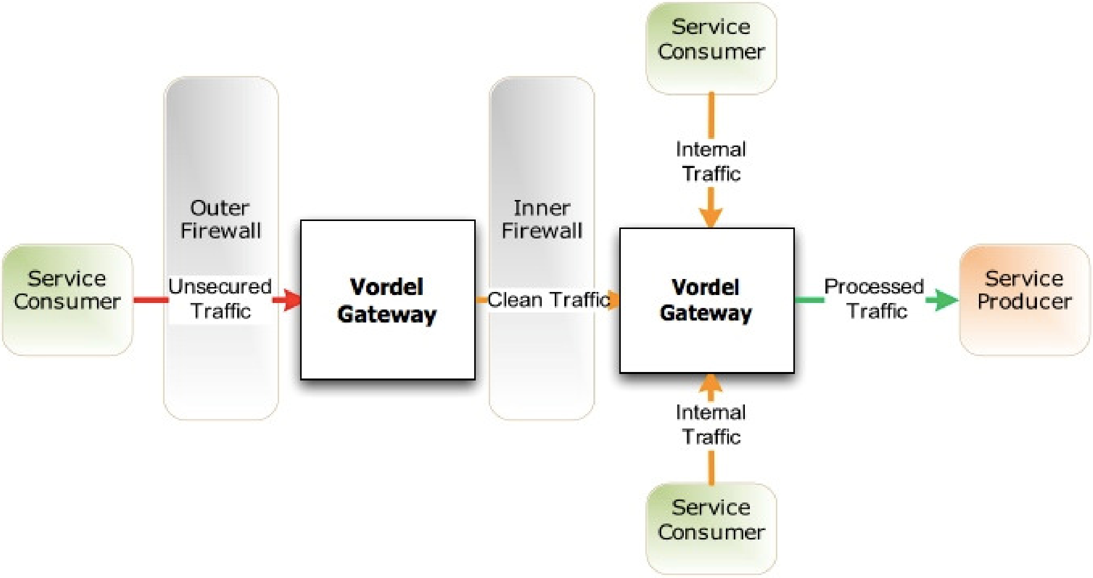


Figure 6: Typical Deployment Diagram

Here are some guidelines to help you make a decision:

- If you are processing only traffic from external sources, consider locating the Gateway in the DMZ. If the Gateway is also processing internal traffic, consider locating it in the LAN.
- If you are processing traffic internally and externally, a combination of Gateways in the DMZ and internally on the LAN is considered best practice. The reason for this is that different policies should be applied to traffic depending on its origin.
- Both internal and external traffic should be checked for threats and to make sure that they correspond to service definitions (WSDL), or for RESTful requests, contain the right parameters.
- External traffic carries a greater potential risk and should be scanned by the Gateway located in the DMZ to make sure that it does not in any way affect the performance of internal applications.

- Internal traffic and pre-scanned external traffic should then be processed by the Gateway located in the LAN. This type of checking includes:
    - WS standards support
    - Checking of service level agreements and enforcing throttle threshold levels
    - Integration with a wide range of third-party systems

7 Securing the Last Mile

Securing the last mile deals with preventing internal users from directly accessing services without going through the Gateway. This can be achieved in multiple ways. You should choose carefully which option is best for your use case, taking into account the security level you want to achieve, and the impact on performance the solution will have:

- *By controlling traffic at the network level*: services can only be accessed if the traffic is coming from pre-approved IPs. This is the simplest solution to put in place, is very secure, and has no impact on performance or existing applications.
- *By establishing a mutual SSL connection between the Gateway(s) and the services*. This solution is the easiest to put in place and has little to no impact on existing applications. However, it does have a non-negligible impact on latency.
- *By passing an authentication token (WS-Security, SAML, and so on) from the Gateway to the back-end services*. This solution has a low impact on latency but requires some development, because the target services container needs to validate the presence and the contents of the token.

For more information about setting up Mutual SSL in the Vordel Gateway, see the *SSL Integrity and Confidentiality* guide on the Vordel Extranet (`extranet.vordel.com`).

8 Planning for Installation

One of the most important tasks when deploying Gateways is confirming that the system is fit for purpose. Modern software systems are hugely valuable to businesses and to the overall success of the business operation. The implications of system downtime are manifold for any organization with important consequences to contend with. The most important factors to look at when architecting a Gateway deployment are:

- What type of policies will run on the system?
- What type of traffic will the Gateway be required to process?
- What is the expected distribution of the traffic?
- How important is the system, and does it need to be always available?
- How to make changes to the system without incurring system outage
- Planning for outage and disaster recovery

8.1 Policies Development

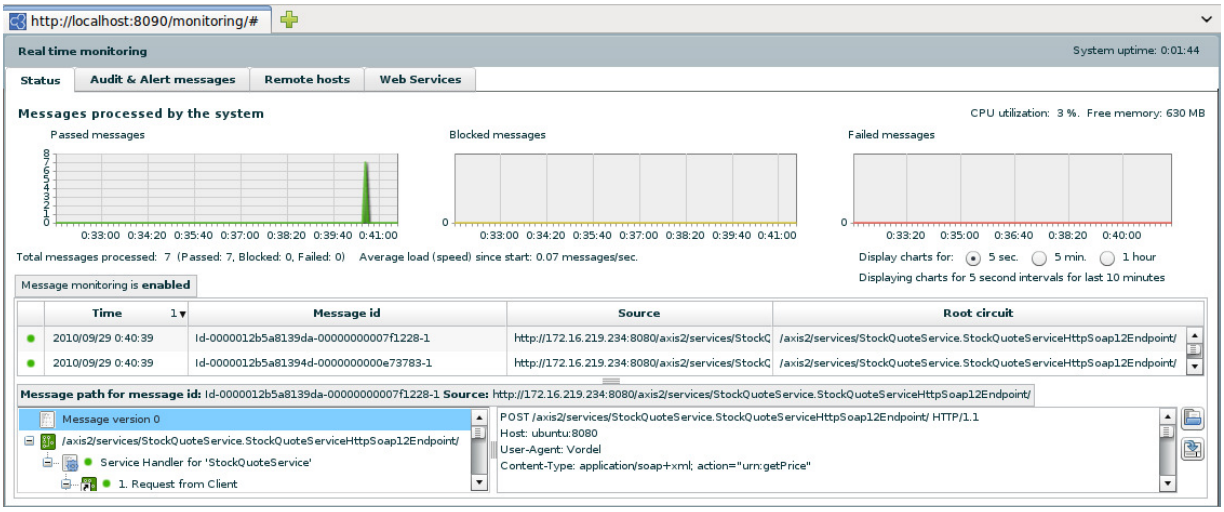
The functional characteristics of any given policy run by a Gateway can have a huge effect on the overall system throughput and latency times. Dependent on the purpose of a particular policy, the demand on valuable processing power will vary. The following guidelines apply, in terms of processing power:

- Threat analysis and transport based authentication tasks are relatively undemanding.
- XML processing such as XML Schema and WS-Security username/password authentication are slightly more intensive.
- Calling out to third-party systems is expensive due to network latency.
- Cryptographic operations like XML Encryption and XML Signature are processor intensive.

The lesson here is that policy performance is conditional upon the underlying requirements, and customers should test their policies prior to deployment into production.

Guidelines

- Decide what type of policy you need to process your traffic. Think in terms of functional requirements instead of technologies. Vordel can help map the technologies to the requirements for you. Examples of functional requirements include: "only trusted clients should be allowed send XML into the network", and "an evidential audit trail should be kept".
- Think about what you already have in your architecture that could help achieve these aims. Examples include LDAP directories, databases that already have replication strategies in place, and network monitoring tools.
- Create a policy to match these requirements and test its performance. Vordel provides an integrated performance testing tool (Vordel SOAPbox) to help you with this process.
- Consider using Vordel Policy Director to manage policies across a whole XML network infrastructure, including multiple Gateways. This will make the migration from test to production much easier to manage.
- Use the Vordel Real Time Monitoring console to help identify what the bottlenecks are in your system. If part of the solution is slowing the overall system, try to find alternatives to meet your requirements.
- View information on network usage using Vordel Reporter.
- Test the performance capability of backend Web Services.



System uptime: 0:01:44

Messages processed by the system

CPU utilization: 3 %. Free memory: 630 MB

Total messages processed: 7 (Passed: 7, Blocked: 0, Failed: 0) Average load (speed) since start: 0.07 messages/sec.

Display charts for: ● 5 sec. ○ 5 min. ○ 1 hour

Displaying charts for 5 second intervals for last 10 minutes

Message monitoring is **enabled**

	Time 1▼	Message id	Source	Root circuit
●	2010/09/29 0:40:39	Id-0000012b5a8139da-00000000007f1228-1	http://172.16.219.234:8080/axis2/services/StockQ	/axis2/services/StockQuoteService.StockQuoteServiceHttpSoap12Endpoint/
●	2010/09/29 0:40:39	Id-0000012b5a81394d-0000000000e73783-1	http://172.16.219.234:8080/axis2/services/StockQ	/axis2/services/StockQuoteService.StockQuoteServiceHttpSoap12Endpoint/

Message path for message id: Id-0000012b5a8139da-00000000007f1228-1 **Source:** http://172.16.219.234:8080/axis2/services/StockQuoteService.StockQuoteServiceHttpSoap12Endpoint/

```
Message version 0
⊟ /axis2/services/StockQuoteService.StockQuoteServiceHttpSoap12Endpoint/
  ⊟ ● Service Handler for 'StockQuoteService'
    ⊟ ● 1. Request from Client
```

```
POST /axis2/services/StockQuoteService.StockQuoteServiceHttpSoap12Endpoint/ HTTP/1.1
Host: ubuntu:8080
User-Agent: Vordel
Content-Type: application/soap+xml; action="urn:getPrice"
```

Figure 7: Real Time Monitoring Console

Example

Supplier A is creating a service that will accept Purchase Order (PO) documents from customers. The PO documents are formatted using XML. The functional requirements are:

- The service should not accept anything that will damage the PO system.
- Incoming XML messages must to be authenticated against a customer database to make sure they come from a valid customer account.
- The supplier already has an LDAP directory and would like to use it to store the customer accounts.
- The supplier must be able prove that the message came from the customer.

These requirements can be achieved using a policy that includes XML Threat processing, and an XML Signature Check, which verifies the certificate against the LDAP Directory.

8.2 Traffic Analysis

In the real world, messages do not arrive in a continuous stream with a fixed size like a lab-based performance test. Traffic distribution has a major impact on system performance. Some of the questions that need to be answered are:

- Is the traffic smooth or does it arrive in bursts?
- Are the messages all of the same size? If not, what is the size distribution?
- Is the traffic spread out over 24 hours or only during the work day?

Guidelines

- Take traffic distribution into account when calculating performance requirements.
- If traffic bursts cause problems for service producers, consider using the Gateway to smooth the traffic. There are a number of techniques for doing this.
- Take message size distribution into account when running performance tests.

8.3 High Availability

Vordel products are used in high value systems, and customers typically deploy them in High Availability (HA) mode to protect their investment.

The design of Vordel products makes this process relatively easy:

- Vordel Policy Director provides policy synchronization. It ensures that all Gateways in a High Availability cluster have the same policy versions and configuration
- Gateways are stateless by nature. No session data is created, and therefore there is no need to replicate session state across Gateways. However, Gateways can maintain cached data, which can be replicated using a peer-to-peer relationship across a cluster of Gateways.
- Gateways are usually deployed behind standard load balancers which periodically query the state of the Gateway. If a problem occurs, the load balancer redirects traffic to the hot standby machine.
- If an SNMP or syslog event is triggered, the issue can be identified using Vordel Reporter and the active Gateway can be repaired.

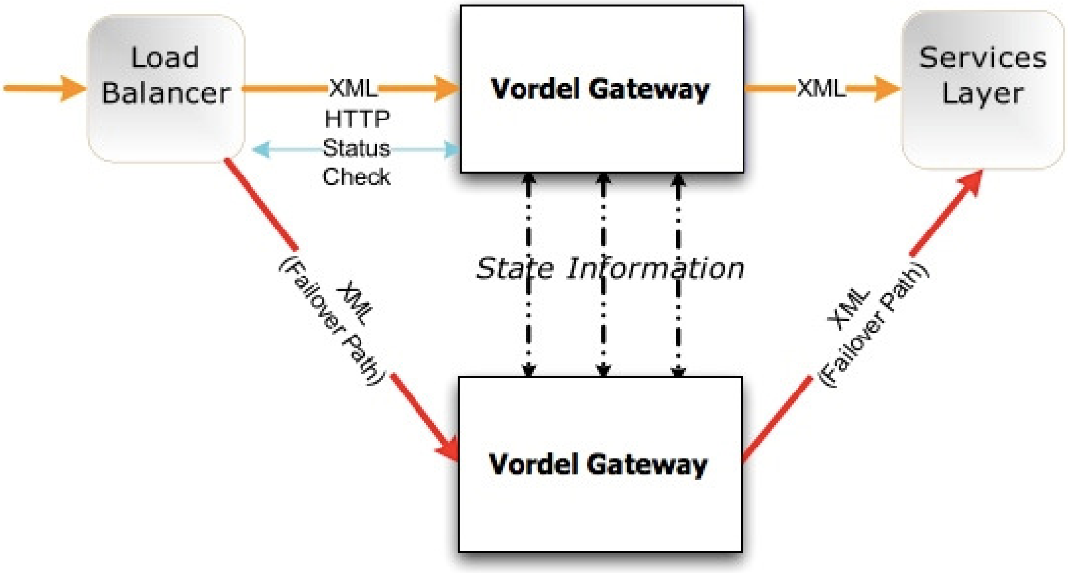


Figure 8: Hot Standby Deployment

High Availability can also be maintained using hot, cold, or warm stand-by systems:

- Cold standby: system turned off.
- Warm (or passive) standby: system operational but not containing state.
- Hot (or active) standby: fully operational and with current system state.

Guidelines

- For maximum availability, Vordel advises the use of a Gateway in hot standby for each production Gateway.
- Use Gateways to protect against malicious attacks that undermine availability.
- Limit traffic to backend Web Services to protect against flooding. This is particularly important with legacy systems that have been recently service-enabled. Legacy systems may not have been designed for the traffic patterns to which they are now subjected.
- Monitor SOA infrastructure carefully to identify issues early. Vordel Reporter and the Real Time Monitoring console enable this. Interfaces are also provided to SNMP and syslog.

8.4 Load Balancing and Scalability

Vordel scales well both horizontally and vertically. Vordel customers scale horizontally by adding more Gateways to a cluster and load balancing across it using a standard load balancer.

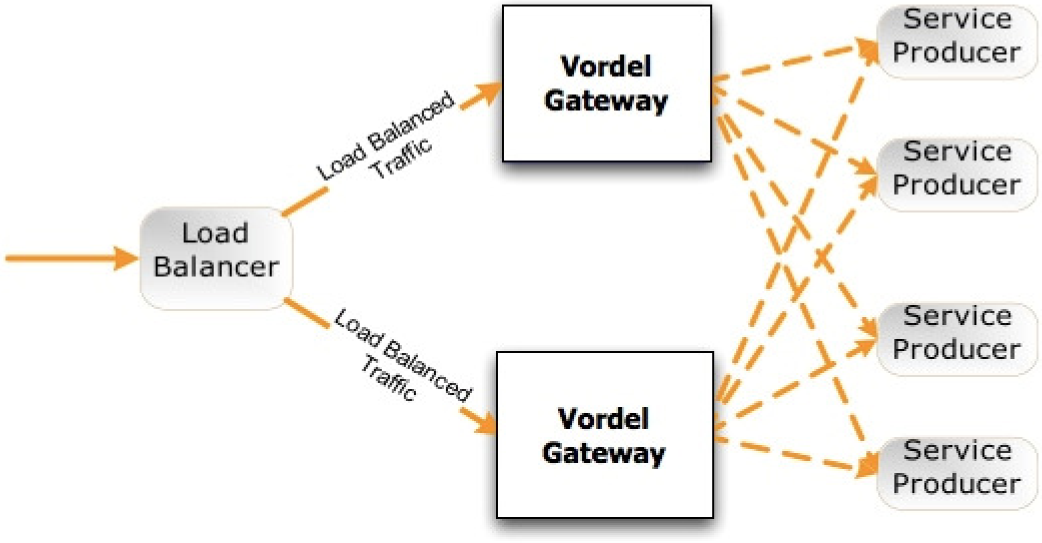


Figure 9: Load Balanced Traffic

The Gateway imposes no special requirements on load balancers. Loads are balanced on a number of characteristics including the response time or system load. The execution of Vordel policies is stateless, and the route through which a message takes on a particular system has no bearing on its processing. Some items such as caches and counters are held on a distributed cache, which is updated on a per message basis. As a result, Gateways can operate successfully in both sticky and non-sticky modes.

The distributed state poses a number of questions for active/active versus active/passive clustering: if the counter and cache state important, you must design your overall system so that at least one Gateway is active at all times. So for a resilient HA system, a minimum of at least two active Gateways at any one time with a third and fourth in passive mode is recommended.

The Gateway itself load balances outgoing messages to backend services using a round-robin or response time-based algorithm. It can also redirect messages to backup systems as a result of connection failures.

For more details on caching setup, see the *Configuring Distributed Caching* white paper on the Vordel Extranet.

Guidelines

- Use Vordel Policy Director to maintain the same policy on load balanced Gateways.
- Configure alerts to identify when Gateways and backend Web Services are approaching maximum capacity and need to be scaled.
- Use Vordel Real Time Monitoring to see what parts of the system are processing the most traffic.

8.5 SSL Termination

SSL connections can be terminated at the load balancer or Gateway level. The Gateway can optionally use a cryptographic accelerator for SSL termination (configured by default on the appliance):

- Connection is terminated at the load balancer level:
    - The SSL certificate (whose subject name is the FQDN of the server, for example, `vordel.com`) and associated private key are deployed on the load balancer, and not on the Gateway.
    - The traffic between the load balancer can be in the clear or over a new SSL connection. The disadvantage of a new SSL connection is that it puts additional processing load on the load balancer (SSL termination and SSL establishment).
    - If mutual (two-way) SSL is involved, the load balancer can insert the client certificate into the HTTP header. For example, the F5 load balancer can insert the entire client certificate (in PEM format) as a multi-line HTTP header named `X-Client-Cert` into the incoming HTTP request. It sends this header to the Gateway, where the Gateway can use it for validation and authentication.
- Load balancer is configured as pass-through: all traffic is passed to the Gateway. With SSL pass-through, the traffic is encrypted so the load balancer cannot make any layer seven decisions (for example, if HTTP 500 is returned by Gateway, route to HA Gateway). To avoid this problem, you can configure the Gateway so that it closes external ports on defined error conditions. Thus the load balancer is alerted to switch to the HA Gateway.

8.6 Disaster Recovery

Most customers have a requirement to keep a mirrored disaster recovery site with full capacity to be able to recover from major incidents. These systems are typically kept in a separate physical location on cold standby until the need arises for them to be brought into action.

Guidelines

- Vordel Policy Director helps get Disaster Recovery sites up and running quicker by pushing out the Gateway policies to the backup solution.
- Remember to include third-party systems in Disaster Recovery solutions.

8.7 Staging and Testing

The most common reason for system downtime is change. Customers successfully alleviate this problem through effective change management as part of a mature software development lifecycle. A software development lifecycle controls change by gradually pushing it through a series of stages until it reaches production.

Each customer will have their own staging policy depending on the value of the service and the importance of the data. Staging can be broken into a number of different milestones. Each milestone is intended to isolate a specific type of issue that could lead to system downtime. For example:

- The development stage is where the policy and service are created.
- Functional testing makes sure the system works as intended.
- Performance testing makes sure the system meets performance requirements.
- System testing makes sure the changes to the system do not adversely affect other parts.

In some cases, each stage is managed by a different group. The number of Gateways depends on the number of stages and requirements of each of these stages.

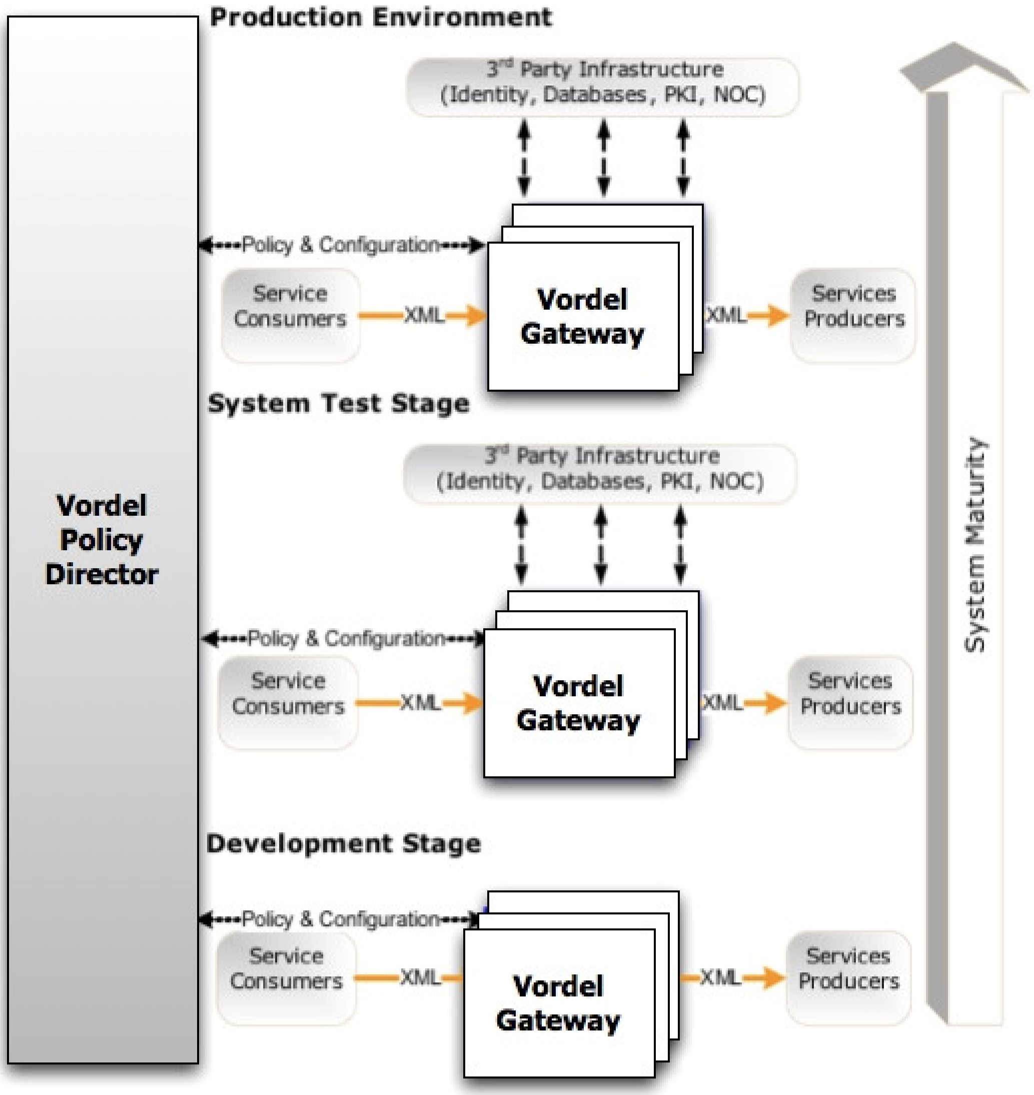


Figure 10: Policy and Configuration Management through Director

Guidelines

- Use Vordel Policy Director to control the migration of policies from development through to production.
- Make sure that only people who are responsible for production systems can make changes to them.
- Keep an audit trail of all system changes.
- Have a plan in place to rollback quickly in the event of a problem occurring.
- Test all systems and policy updates before promoting them to production.
- Test High Availability and resiliency before going into production.

9 How does Vordel Interact with your Existing Infrastructure?

As part of policy execution, the Gateway needs to interact with various parts of the existing such as databases, LDAP servers, or identity management products.

9.1 Databases

Vordel interoperates with both relational and XML database types. Databases may be used for a wide variety of purposes by Vordel Gateway (for example, for access control credentials, authorization attributes, identity and role information, and logging and reporting).

Vordel uses JDBC to connect to databases. Supported databases include MySQL, Oracle, DB2 and SQL server.

9.2 Anti Virus

Vordel supports Anti-Virus (AV) scanning using virus scanning engines from McAfee, Sophos, and ClamAV. Depending on the engine, this scanning can happen in-process or remotely using a client SDK or Internet Content Adaptation Protocol (ICAP). Vordel takes the XML message attachments, passes them to the AV scanner and then acts on the decision.

- AV signature distribution and updates are performed using mechanisms of the antivirus vendor.
- Licensing for the AV engine is done through the AV vendors distribution channels.

9.3 Operations and Management

Vordel has a number of different logging options:

- Audit and reporting logs are detailed logs that are sent to syslog (UDP/TCP), relational databases, or flat files. They contain detailed records of processed messages, what their contents were, how long the processing took, and what decisions were taken during the message processing. This type of logging can also include information alerts about policy execution failures and breached SLAs, along with information about critical events such as connection or disk failures. The logging level can be controlled for a configuration or policy as a whole or on a filter by filter basis. The auditing information can be viewed in real time from the Real Time Monitoring console, but also can be pushed to a database for later analysis using the reporting tools.
- The Real Time Monitoring console is also used to provide a current snapshot of how the XML networking system is behaving. It tells you how many messages are being processed and what services are under the most load. Real Time Monitoring tells you what is happening now on a system, and can be viewed by pointing a browser at the system.
- Flexible alerts are alerts that can be sent out to email, SNMP, OPSEC, syslog, Twitter and Windows Event Log based on a condition being met in a policy. An example might be to email a service owner for every 1000 failures or to generate an alert if a service is processing more than 10000 messages per second. They can also be used to generate alerts on client usage.
- Service Level Agreement filters can be used to carry out a statistical measure of the services quality of service. They are used to make sure that the amount of network connection errors, response times and server errors are below a certain threshold.

9.4 Network Firewalls

When deployed in a DMZ, Vordel sits behind network firewalls. Network Address Translation (NAT) firewall functionality is used on the network firewall to provide the Gateway with a publicly routable address in the DMZ. This allows the Gateway to route traffic internally to a local IP address range. Gateways may be dual-homed to pass messages between the DMZ and the internal, trusted network.

Vordel then carries out security processing over the incoming traffic, which includes:

- Looking for known attack patterns.
- Checking on the validity and structure of the message for anomalies.
- Looking for traffic patterns that suggest a Denial-of-Service (DoS) attack.

Advantages

Gateways have a number of advantages over traditional application firewalls for XML processing:

- They understand the structure of the traffic, and can detect subtle attack mechanisms such as entity expansion attacks and external reference attacks.
- They can consume information in the messages such as security and platform specific tokens.
- They can use well understood standards such as XML Schema, XPath, and WSDL to properly content filter the traffic.

If an attack or unusual traffic pattern is detected, the Gateway can notify the firewall to block the traffic at source using OPSEC or some other notification mechanism.

Firewall Modes

You can configure the Gateway in two modes:

- Block unidentified traffic, which is the default setting. If there is no policy configured for this traffic, block it, and (depending on configuration), raise an alert. In this way, rogue XML traffic is detected and blocked.
- Pass unidentified traffic.

You can configure the Gateway to act as a network endpoint or a network proxy, or both in tandem.

9.5 Application Servers

Application servers are the infrastructure alongside which Vordel Gateways are most commonly deployed. For example, Vordel Gateways are currently deployed in production systems with IBM WebSphere, Oracle WebLogic, Microsoft Biztalk, Fiorano SOA Platform, TIBCO BusinessWorks, and many others.

Vordel products interact with application servers in a number of modes:

- Intercepting application server traffic by acting as a proxy.
- Offloading processing handed over by the application server using service calls (for example, to offload XML transformation, or XML Signature validation).

For increased integration with such systems, the Gateway supports numerous transport protocols including HTTP, HTTPS, JMS , email (SMTP/POP), or FTP.

9.6 Enterprise Service Buses

Gateways and Enterprise Service Buses (ESBs) are similar functionally and complement each other very well. Gateways are used primarily to:

- Protect ESBs and downstream systems from traffic surge, potential DoS attacks, and threats.
- Offload expensive operations such as message validation, cryptography operations from ESBs.

Similarities

- Protocol mediation
- XML routing and transformation
- Service composition
- XML processing

Differences

- Gateways can be used for simple composite services (chained), but do not support Business Process Execution Language (BPEL), and are not suitable for long duration composite services.
- ESBs are usually delivered with a wealth of backend adapters for systems such as CICS, IMS, Siebel, or SAP.
- Gateways are stateless and cannot maintain transaction state.
- Gateways are targeted at performance and application acceleration.
- Gateways have been designed to provide superior security capabilities, without impacting performance.

9.7 Directories and User Stores

Vordel supports a wide variety of user stores including LDAP, Active Directory, and access control products such as CA SiteMinder and Oracle Access Manager.

User Store Usage

Vordel can use LDAP directories to retrieve user information including:

- Authentication using username/password.
- Retrieve certificates for checking XML Signatures.
- Authorization of clients based on attribute values.
- Retrieval of attributes for placing into SAML assertions.
- Checking certificate validity using Certificate Revocation Lists (CRL) retrieved from user stores.

For more information about integration with the LDAP server of your choice, see the various integration guides on the Vordel Extranet (https://extranet.vordel.com/?page_id=13).

Deployment Considerations

User stores contain some of the most valuable information in an organization. They contain private identity information such as phone numbers, addresses, email addresses, medical plan IDs, usernames and passwords, certificates and organization structures. Gateways must be able to interact with user stores without compromising them.

Simple Inline User Store Deployment

The following diagram shows a simple inline user store deployment:

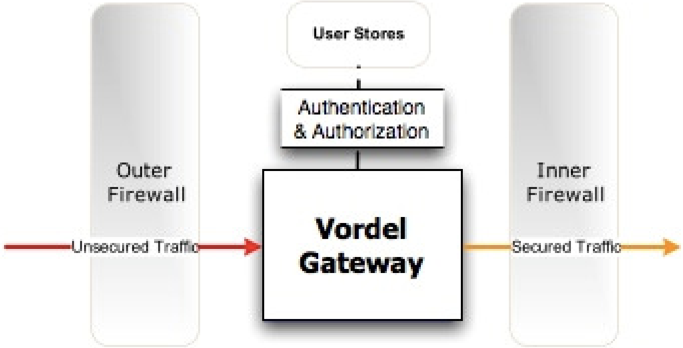


Figure 11: Inline User Store (DMZ)

Advantages

- Simple and easy to setup.
- There is a single entry point through the DMZ for XML traffic.

Disadvantages

- Exposing important user information in the DMZ is a potential security risk.
- LDAP server is only being used for external traffic.

Gateway in DMZ—LDAP in LAN

This is a very common setup where the Gateway is located in the DMZ where it communicates with a user store in the LAN:

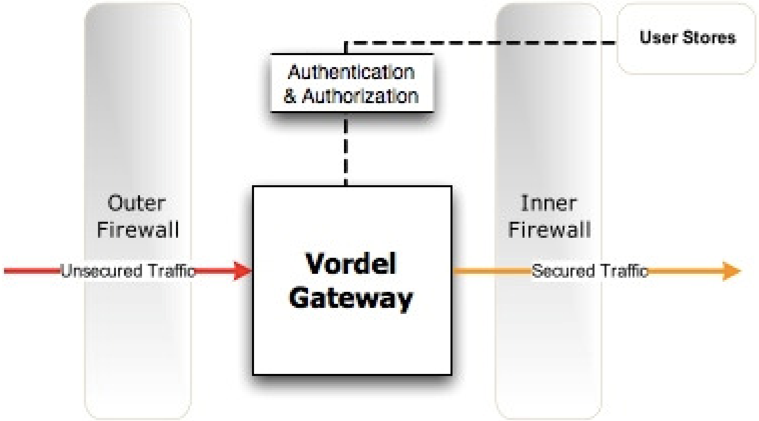


Figure 12: User Store in LAN

Advantages

- User store is protected from external access.

Disadvantages

- Network professionals need to maintain two entry points into the LAN from the DMZ for a single application.
- The user store is addressable from the DMZ, which is contrary to many organization's security policies.

Split Deployment between DMZ and LAN

Two Gateways are used to split the security checks across the DMZ and the LAN. Threats and XML validity are performed in the DMZ, while authentication and/or authorization is performed in the LAN.

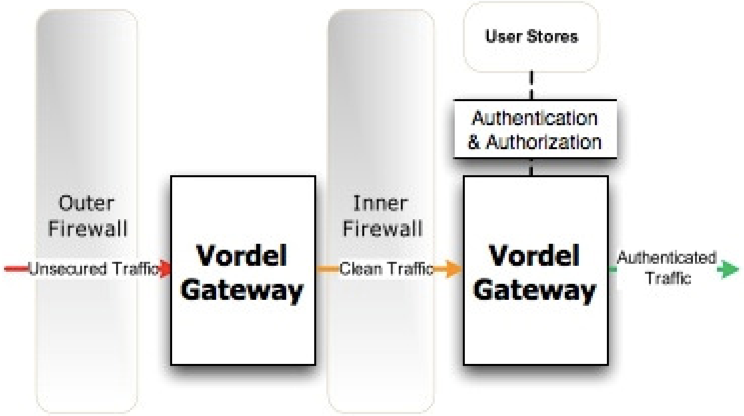


Figure 13: Split Deployment

Advantages

- Most secure deployment available.
- By separating threat from access control, it is easy to run separate security policies for internal and external traffic.
- Policy Director can be used to manage all Gateways

Disadvantages

- This is a more expensive option.

9.8 Access Control

Vordel Gateway interoperates with Access Control products at a number of different levels:

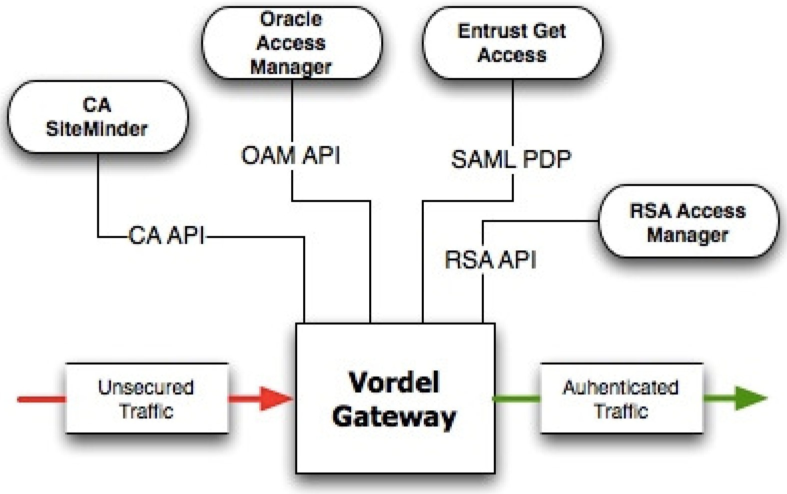


Figure 14: Example Access Control Options

- Vordel Gateway can directly connect into the Identity Management system as an agent. This solution is currently available for Oracle Access Manager, Oracle Entitlements Server, RSA Access Manager, CA SiteMinder, and IBM Tivoli Access Manager. The Identity Management policy is defined in the Identity Management product to which Vordel delegates the authentication and authorization.
- Vordel Gateway can connect to the Identity Manager using the XML Access Control Markup Language (XACML) and Security Assertion Markup Language (SAML) protocols. Vordel can request an authorization decision from a SAML Policy Decision Point (PDP) for an authenticated client using the SAML Protocol (SAMLP), which is defined in XACML. In such cases, Vordel presents evidence to the PDP in the form of user credentials, such as the Distinguished Name of a client's X.509 certificate, or a username/password combination.
- The PDP decides whether a user is authorized to access the requested resource. It then creates an authorization assertion, signs it, and returns it to Vordel in a SAMLP response. Vordel can then perform a number of checks on the response, such as validating the PDP's signature and certificate, and examining the assertion. It can also insert the SAML authorization assertion into the message for consumption by a downstream Web Service. This allows propagation of the access control decision to occur.

9.9 Public Key Infrastructure

Vordel Gateway supports SSL and TLS for transport-based authentication, encryption, and integrity checks. Vordel Gateway can interact with Public Key Infrastructure (PKI) systems in the following ways:

- Connecting to Online Certificate Status Protocol (OCSP) and XML Key Management Specification (XKMS) to query certificate status online.
- Using a Certificate Revocation List (CRL) retrieved from a directory, file, or LDAP to check certificate status.
- Checking a certificate chain.

Certificates and keys can be stored in the Gateway keystore, or in a network or an optional Hardware Security Module (HSM).

9.10 Registries and Repositories

Vordel Gateway supports the following:

- Vordel Policy Studio can pull Web Service Definitions (WSDL) from UDDI directories or HTTP-based repositories.
- These WSDL files are then used to generate security policies.
- Vordel Gateway can update registries with updated WSDL files or can serve them directly to the client.

To learn more about integration with your registry, see the integration guides available from https://extranet.vordel.com/?page_id=13.

10 Conclusion

This document describes how the Vordel Gateway fits in an enterprise deployment, and how it can be used to secure and accelerate the deployment of services or APIs.