



CASOS DE USO DE VORDEL EM TELECOM

Vordel XML como Firewall – Proteção contra ameaças a Aplicações XML como ameaças de ataques maliciosos e acesso não-autorizado

Vordel XML como Gateway – Para uso em Redes em Nível de Aplicação com descarga de funções XML com transformação de dados, roteamento e aceleração

Vordel Policy Director – Gerenciamento e criação centralizado de Políticas para redes de firewalls e gateways XML

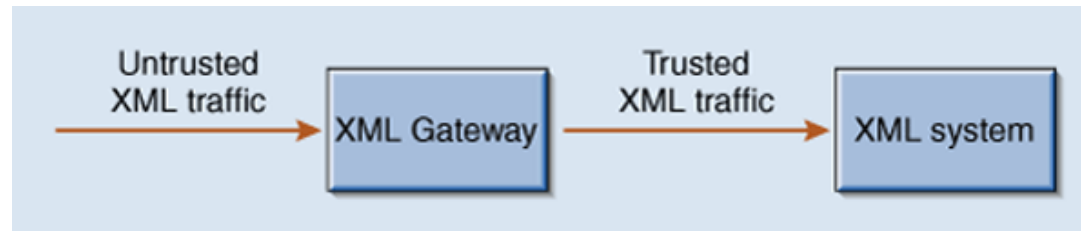
Vordel Reporter – Relatórios e Métricas com total visibilidade da utilização de Web Services

Vordel SOAPbox – Ferramenta de Testes para Aplicações XML e de Web Services

GATEWAYS XML: ARQUITETURA



- > Arquiteturalmente, um **Gateway XML** é um proxy reverso à frente dos Web Services



- > “Virtualização de Serviços”
 - > Os Web Services são protegidos do acesso direto
 - > Web Services podem ser renomeados, movidos para diferentes plataformas ou ser alterados, porém o Gateway irá ocultar isto.
 - > Clientes diferentes podem ser direcionados para Serviços diferentes [“Clientes Ouro” utilizando um serviço, enquanto “Clientes Prata” utilizariam outro]
 - > Aceleração de Aplicações
 - > Reduz a carga de Processamento XML sobre o Application Server
 - > Análise do Tempo de Resposta dos Serviços
 - > Latência ou Serviços Indisponíveis são relatados imediatamente.
-

Roteamento baseado no Conteúdo

- > Exemplo: Mensagens em conformidade com o ACORD v2.0 são enviadas para um destino enquanto mensagens em conformidade com o ACORD v1.5 são direcionadas para outro destino.

Controle de Tráfego

- > Se um Web Service pode apenas atender X mensagens/segundo, então um Gateway XML pode controlar o tráfego e limitá-lo a este nível.
- > Se o cliente apenas pagou por X mensagens/segundo, então um Gateway XML pode limitar sua utilização a este nível



- > Transformação de mensagens em diferentes formatos

Reforço das Regras de Controle de Acesso

- > Controle sobre qual cliente pode acessar qual Web Service
 - > Conexão com Gerenciamento de Identidade: CA SiteMinder, RSA, Sun, Novell
-

Mediação de Protocolo

- > Exemplo: XML Mensagens são recebidas pelo protocolo HTTP e então colocadas em uma fila JMS

Log da utilização de Web Services

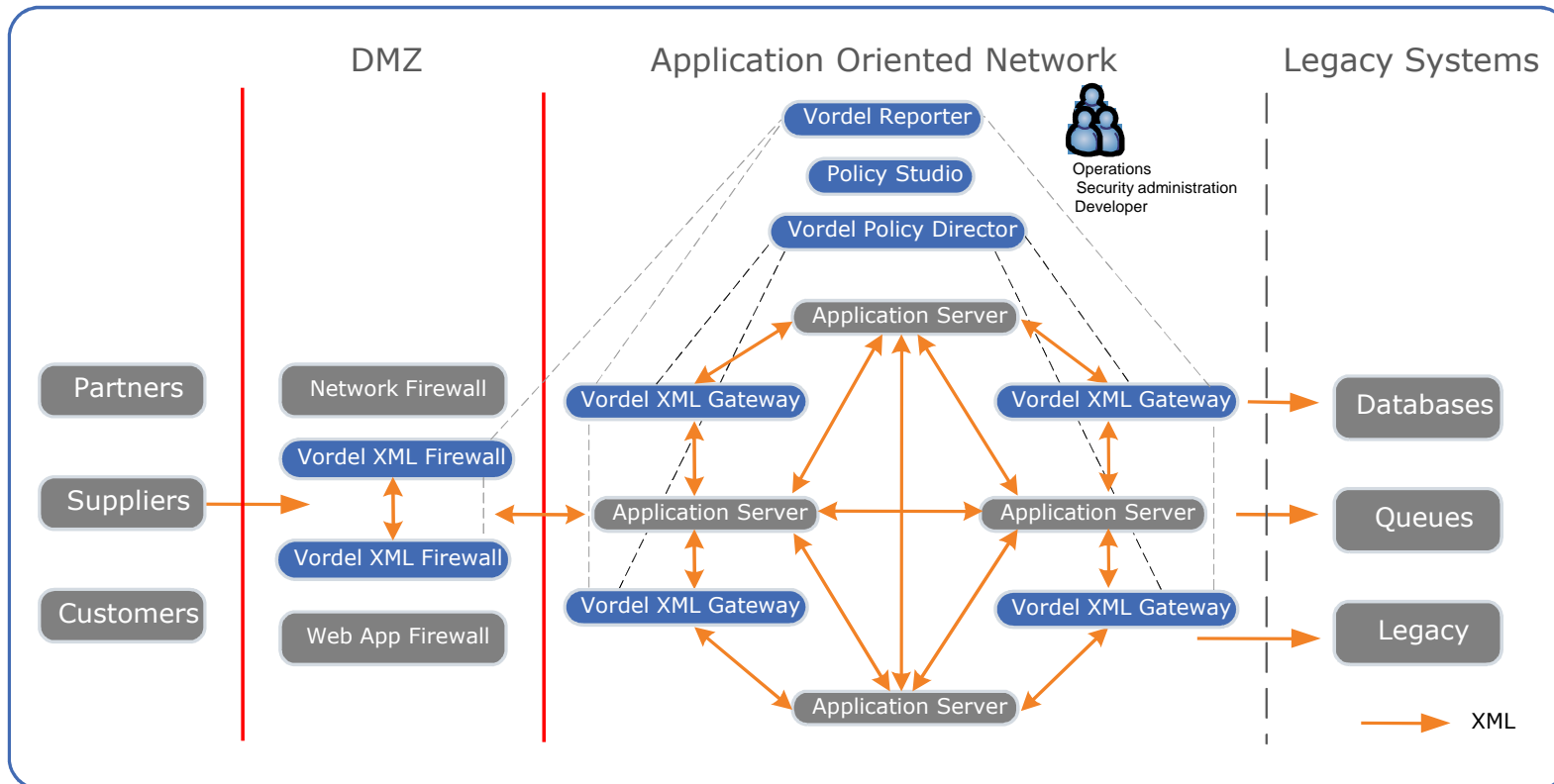
- > Tempos de Resposta
- > Quais serviços são mais utilizados
- > Quais clientes acessam quais serviços
 - > Eventos de Segurança

Proteção contra ameaças no dados XML e anexos SOAP

- > Análise de Tamanho de Mensagens
 - > Validação de Schema
 - > Varredura de anexos SOAP
- > Detecção de ataques como SQL Injection



VORDEL



Proteção para aplicações XML contra ataques maliciosos e acesso não-autorizado

- > Prevenção de ameaças
 - > Ataques Clogging, serviço de scanning, XML DoS, Data harvesting, injeção SQL , vulnerabilidades com parsers XML, frameworks .Net e J2EE
- > Autenticação de Cliente
 - > certificados HTTP-Auth, X.509, Perfil de Segurança WS-I Basic
 - > Alertas para eventos de Segurança
- > *Lista negra* com firewalls de rede
- > Validação de dados
 - > Validação de mensagens contra XML Schemas e perfil WS-I Basic
- > Rápida Implantação
 - > Políticas pré-carregadas
- > Segurança para qualquer tipo de aplicação XML
 - > SOAP, Plain XML, REST
- > Trilhas de Auditoria
- > Monitoramento em Tempo Real



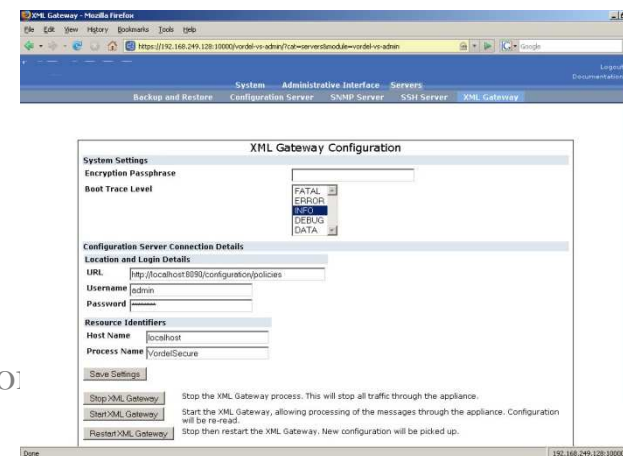
- ✓ Manipulação de tráfego XML e processamento de acordo com políticas.
- ✓ Integração, Aceleração, Enriquecimento de XML, Garantia de Níveis de Serviço, Mediação de Protocolos e Operação em Redes XML
- ✓ Suporte a Padrões como WS Security, Encriptação XML, Assinaturas XML, WS Trust, SAML e Endereçamento XML
- ✓ Todas as funções do XML Firewall, para evitar o acesso de tráfego suspeito a Web Services:
 - Proteção para tráfego XML
 - Detecção de Ameaças XML
 - Controle de Acesso
 - Entre outros

Redes em Nível de Aplicação

Descarga de funções XML com transformação de dados, roteamento e aceleração

- > Facilidade de Implantação
 - > *Appliance* que não requer instalação
- > Aceleração de Aplicações
 - > Descarga de funções XML pesadas dos servidores de aplicação para o motor de aceleração interno VXA
- > Roteamento
 - > Roteamento condicional baseado em ID, conteúdo e tipo de conteúdo para aplicações
- > Gerenciamento de Identidade
 - > Suporte a infra-estrutura IAM para autenticação e autorização de tráfego XML

- > Mediação de Identidade
 - > Mediação de identidade entre diferentes esquemas de segurança
- > Desempenho
 - > Motor de aceleração XML patenteado **VXA** em conjunto com aceleração de criptografia
- > Virtualização de Serviços
 - > Proteção a pontos de acesso contra acesso direto
- > *Traffic Throttling*
 - > Proteção contra picos de tráfego não previstos
- > Enriquecimento de Dados
 - > Popular conteúdo em documentos XML a partir da o



➤ Monitoração e relato de uso de Web Services

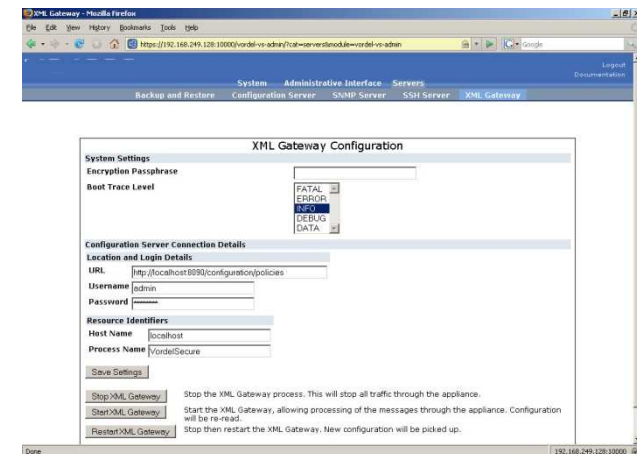
➤ Integração com registros UDDI

➤ Service Manager: ferramenta

que permite definir Políticas

a serem aplicadas aos Web

Services

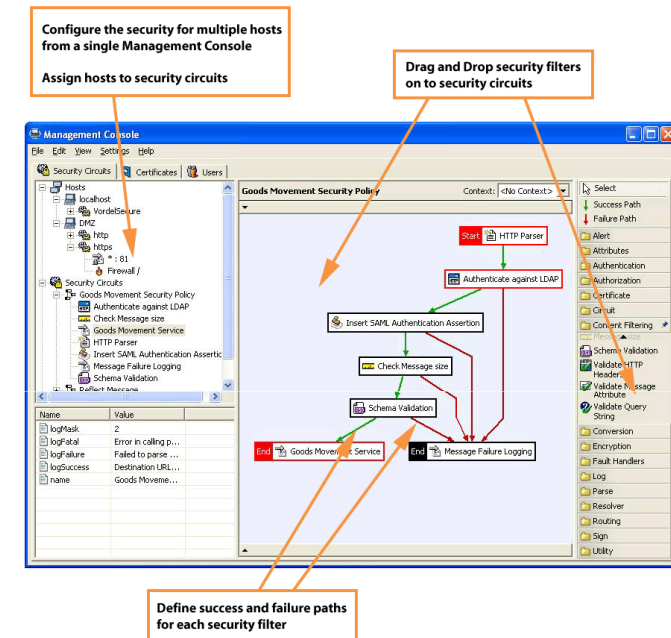


VORDEL POLICY DIRECTOR



Política Centralizada de Gerenciamento para rede de Gateways XML and Firewalls XML

- > Política para Gerenciamento de Tempo de Vida
 - > Simplifica a migração através do desenvolvimento, teste, validação e na implantação em produção
- > Logs Centralizados
 - > Armazenamento de todas métricas para análise posterior
- > Política de Armazenamento Flexível
 - > LDAP, Bancos de Dados Relacionais e XML ou file system
- > Rápida Replicação da Rede de Infraestrutura XML
 - > Facilidade para a rápida criação de novos gateways e firewalls
- > Rastro Auditável de Políticas
 - > Arquivamento de todas transações relacionadas em suas Políticas
- > Provisionamento de novos Gateways XML e distribuição de Políticas

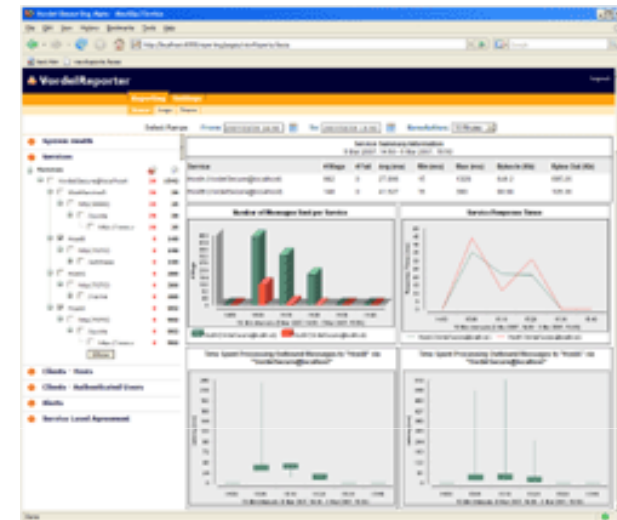


VORDEL REPORTER



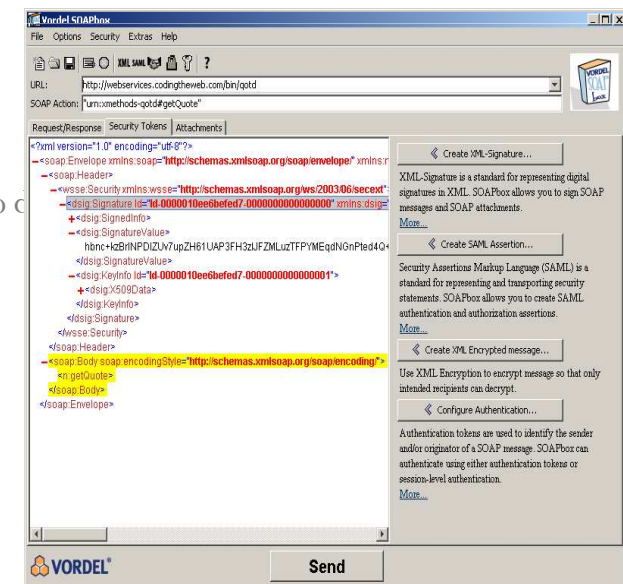
Visão complete das informações sobre seus Web Services através de Relatórios customizáveis

- > Tela de Relatórios Customizável
- > Análise de Uso dos Serviços
 - > Rastreie e analise o uso dos Serviços
- > Avaliação de Performance
 - > Rastreie latências, tempos de resposta e alertas de erro
- > Tuning dos níveis do Serviço e thresholds
 - > Optimize o nível dos serviços e a performance individual destes
- > Auditoria e logging
 - > Interface para gerar relatórios sobre todas transações dos Web Services
- > Causa Raiz - Análise de dados
 - > Determine gargalos nos Serviços e anomalias
- > Relatório de Gerenciamento de Excessões
 - > Relatório de ocorrências fora do normal/padrão do Serviço



Teste de Performance, escalabilidade e segurança dos Web Services

- > Teste de Stress de Web Services antes do deploy
- > Mensagens SOAP de exemplo
 - > Inicio rapido com mensagens já criadas
- > Configure a Encriptação/Desencriptação XML
 - > Simplificação destas funções
- > Inclusão/Remoção automática de Marcadores de Segurança
 - > Inserção/Remoção automática de marcadores para acelerar o processo de testes
- > Adiciona anexos SOAP facilmente
- > Índice de chaves Gráfico
 - > Carregue várias chaves e certificados digitais sem a utilização de ferramentas de linha de comando



- O Vordel foi construído pensando, na velocidade de processamento de XML e nas funções que acumula como encriptação, autenticação, anti vírus etc. Por isso apresenta um motor VXA para acelerar o processamento e manipulação de XML.
- Aceita hardwares de alta qualidade, além de uma placa aceleradora para manipular todas as operações de criptografia e SSL.
- O Vordel Gateway VX4000 processa até 10 vezes mais tráfego XML que uma aplicação padrão como BEA, IIS, WebSphere, etc. Especialmente em se tratando de funcionalidades de segurança como WS Security, SAML, encriptação, assinaturas, etc..
- Encriptação e autenticação: quando feita no XML Gateway ao invés do ESB, esta função tem uma aceleração de mais de 15 vezes. Há casos em que se passou de 8 para 200 transações por segundo, apenas se fazendo o *off-load* de funções do ESB.
- Ganha-se em média 4 vezes em desempenho quando se retira XML Schema, XSLT, XML Signature e encriptação XML do servidor de aplicação e se colocam estas funções num *appliance* VS4000 XML Gateway.

CENÁRIOS DE USO



Telecoms

- > Enriquecimento em voo de XML, obtendo informações de assinantes, dos databases
- > Plataforma de Serviço de Segurança de Entrega (SDP)
- > Dimensionamento de Trafego, proteção de excesso de trafego XML nos servidores de aplicação

Financial Services

- > Aceleração de conteúdo XML
- > Aplicação de PKI e RBAC ao trafego XML
- > Criar um canal seguro de integração para bancos e seguradoras

Setor Publico

- > Submissão de privacidade de dados compliance através de determinadas trilhas de auditoria
- > Aceleração de offload XML

Manufacturing

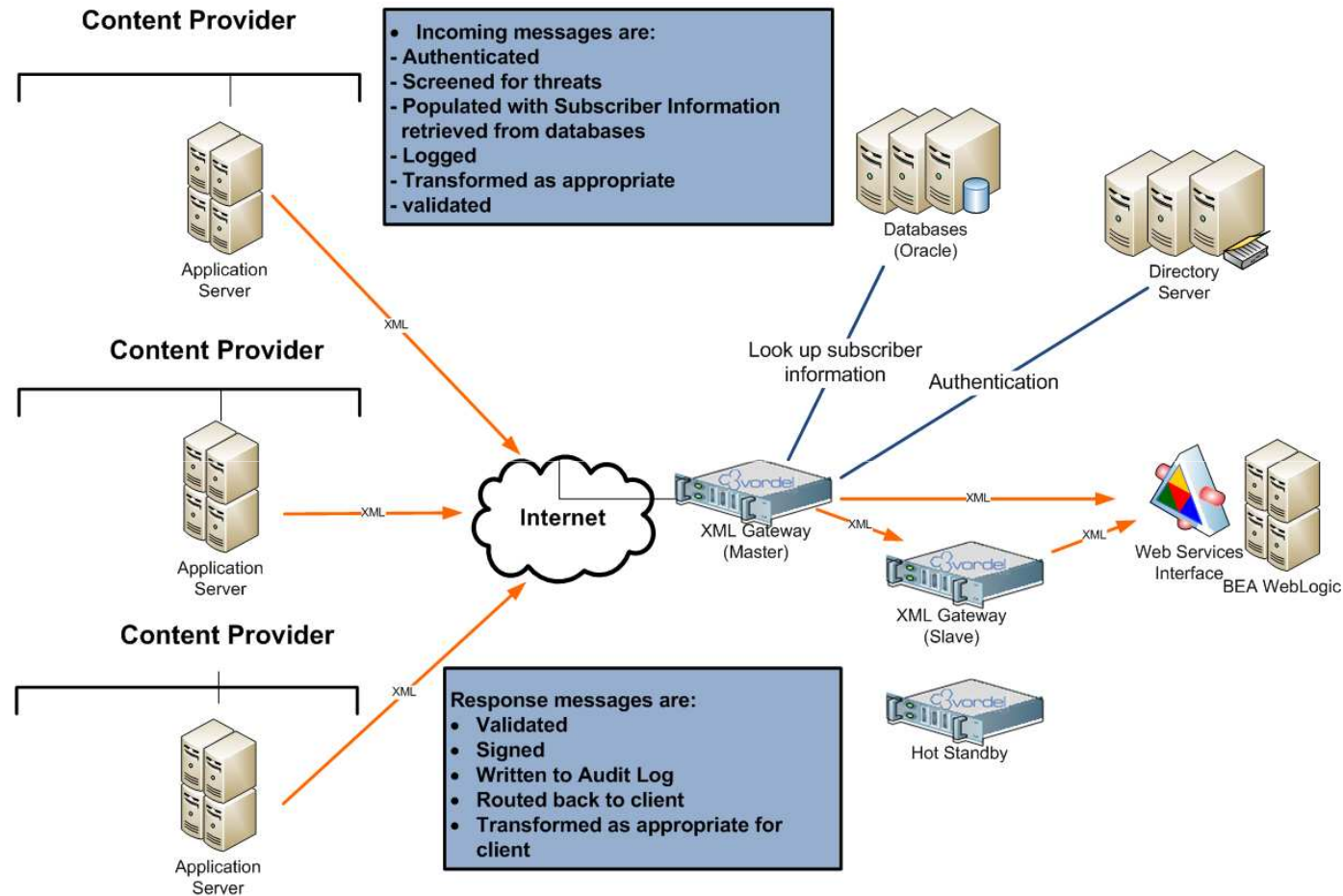
- > Conexões seguras para a cadeia de suprimentos
- > Ligar firmas de logística a fabricantes

- ✓ Estudo de Caso 1: Service Delivery Platform (SDP) em Operadora Celular [Brasil]
- ✓ Estudo de Caso 2: Serviços de Emergência 911 [EUA]
- ✓ Estudo de Caso 3: Desregulamentação [Canadá]
- ✓ Estudo de Caso 4: Gerenciamento de IPTV [Itália]
- ✓ Estudo de UTMS
- ✓ Estudo de caching
- ✓ Estudo de VAS
- ✓ Estudo de Broker

Os produtos Vordel são um importante componente da “Service Delivery Platform” da Ericsson que utiliza o XML para conectar sistemas de telecoms

- Parlay-X é o padrão XML utilizado
- Vordel XML Gateway faz a validação do tráfego Parlay-X
- Vordel XML Gateway também oferece consulta a informações de assinantes em bancos de dados, e população “em vôo” de dados de assinantes em campos XML nas mensagens Parlay-X XML

ARQUITETURA DA SOLUÇÃO



O cliente oferece serviços externos de telefonia de emergência tanto para provedores de linhas fixas quanto de VoIP incluindo Verizon e Vonage

Informações do cliente são alimentadas ao provedor do serviço 911 utilizando XML

A mensagem XML inclui:

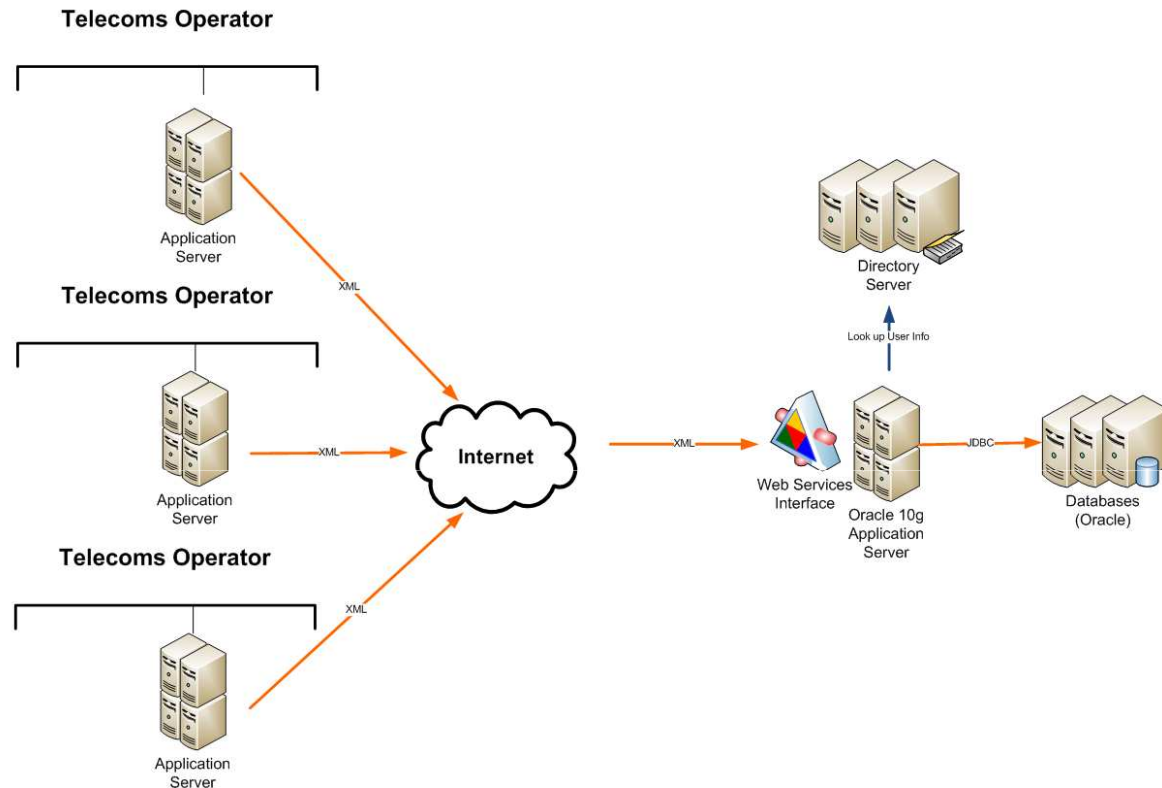
- Nome
- Endereço
- Idioma Preferido

Quando o cliente disca 911, esta informação é fornecida aos serviços de emergência [polícia, bombeiros, ambulância].

O cliente recebe um *feed* regular desta informação de clientes. *Feeds* podem conter milhões de detalhes de clientes individuais.

1) Operator sends customer information as XML
2) Application Server processes XML slowly
3) Operator re-sends the message when it does not get an immediate response

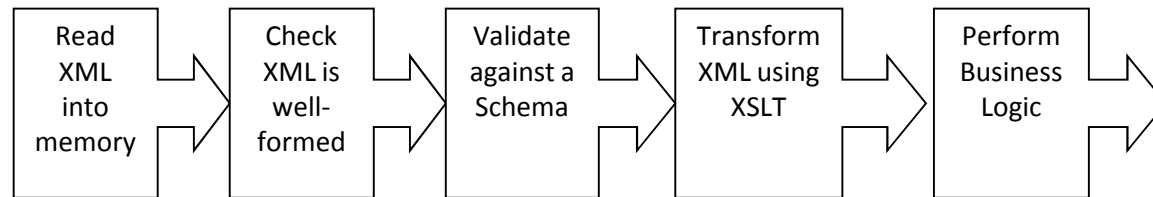
1.O operador envia a um cliente uma informação como XML
2.O servidor de aplicação processa vagorosamente o XML
3.O operador reenvia a mensagem quando não tem uma resposta imediata



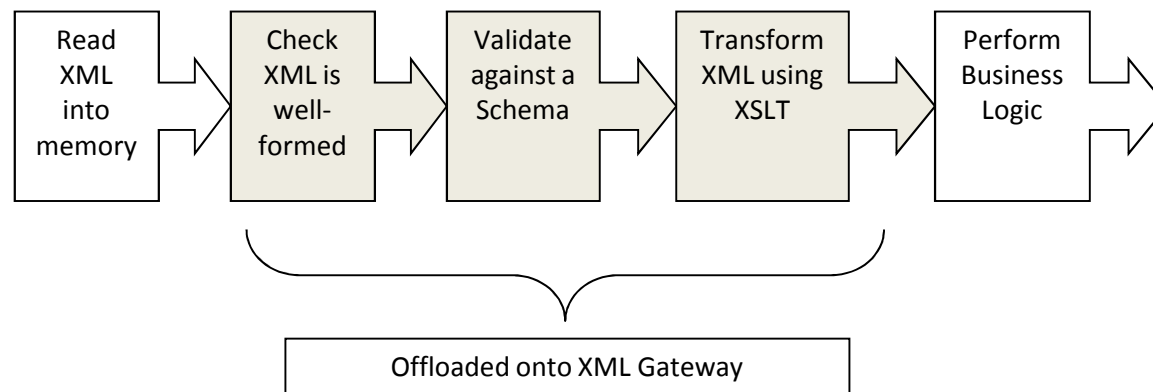
Código Java no Oracle Application Server estava validando o XML de entrada, e autenticando o remetente. Infelizmente, sua execução era lenta e falhava sob grande demanda.

Vordel XML Gateway tira do servidor de aplicação o pesado processamento XML

- **Antes:**



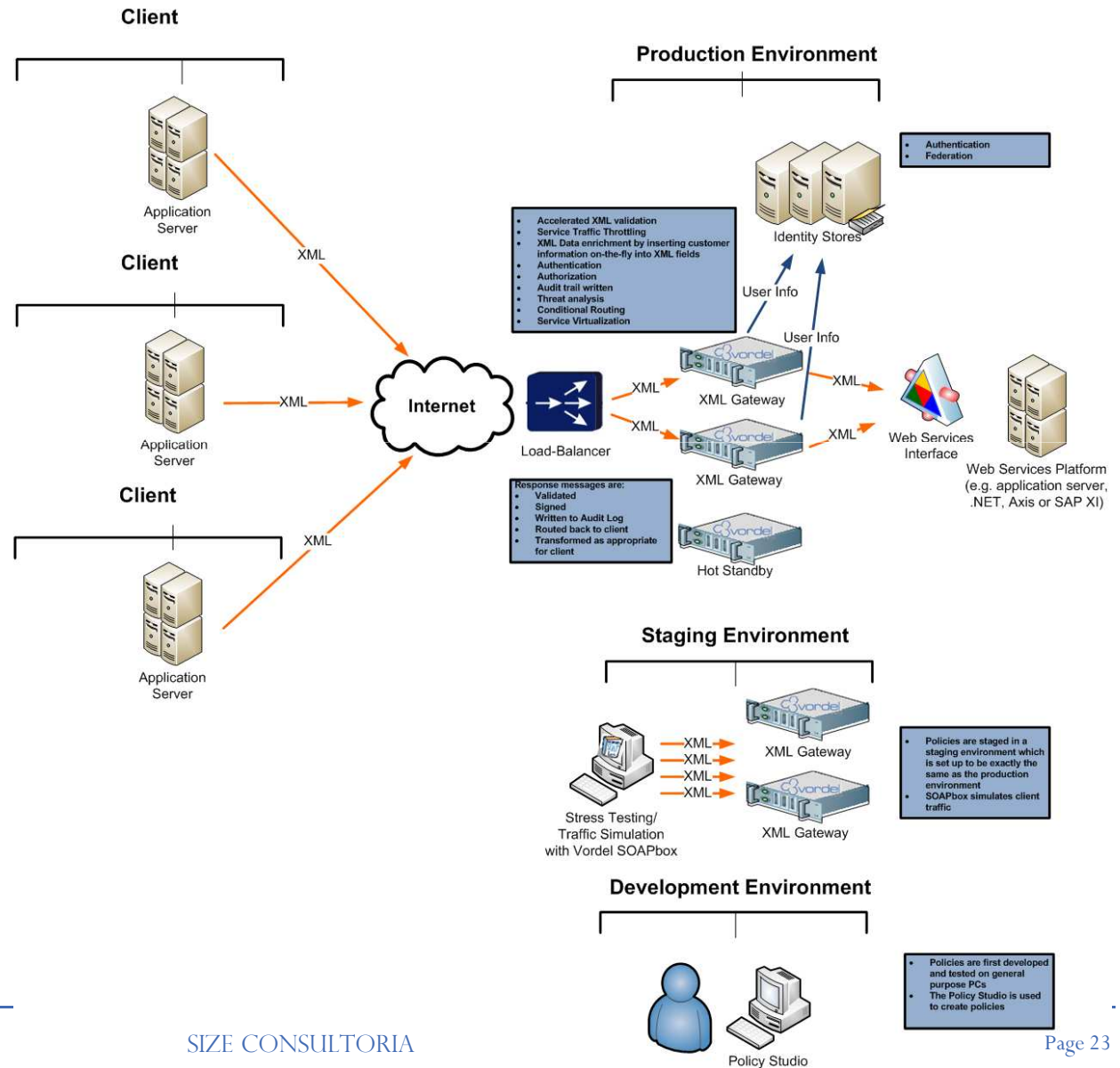
- **Depois:**



ARQUITETURA DA SOLUÇÃO



- Failover
- Desenvolvimento, Teste e produção
- Os processos pesados de XML feitos for a dos servidores de aplicação

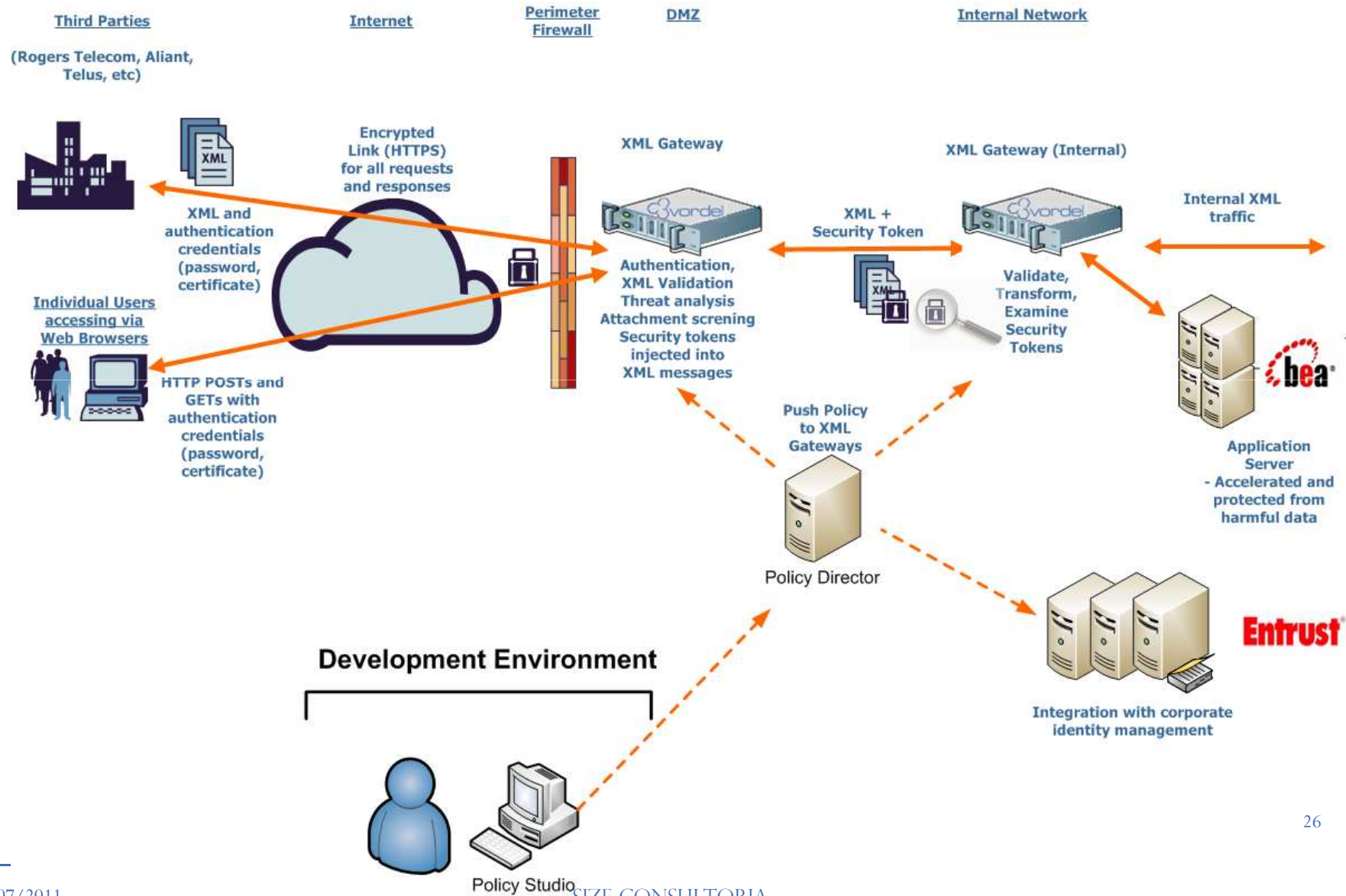


- Reenvios de mensagem são automaticamente detectados e bloqueados
- Respostas são mantidas em *cache* de modo que mensagens reenviadas não precisam acessar o servidor de aplicação
- XML é validado e verificado contra ameaças antes de chegar ao servidor de aplicação
- Políticas de segurança agora estão nas mãos da equipe de Operações
- Políticas não são mais incluídas em código no servidor de aplicação
- Back-up, roll-back, atualização e arquivamento de políticas
- Trilha de auditoria de evidências (assinada) completa é fornecida

Maior companhia de telecomunicações canadense oferece conectividade a clientes residenciais e corporativos.

- Necessário oferecer conectividade com CLECs (Competitive Local Exchange Carriers) em um ambiente de telecoms de-regulado
- Tinham um portal web existente que dava acesso a CLECs a informações usando um navegador web. Mas queriam um acesso B2B automatizado usando XML.
- 500.000 usuários de portal, com mais 5.000 sendo adicionados por mês
- Lançamento de novos serviços B2B XML Web Services, juntamente ao portal, para permitir que clientes e parceiros maiores integrem seus sistemas de *back office* diretamente aos sistemas do provedor de telecom
- Produtos Vordel integrados com Web SSO (Entrust) e Enterprise AV (McAfee).

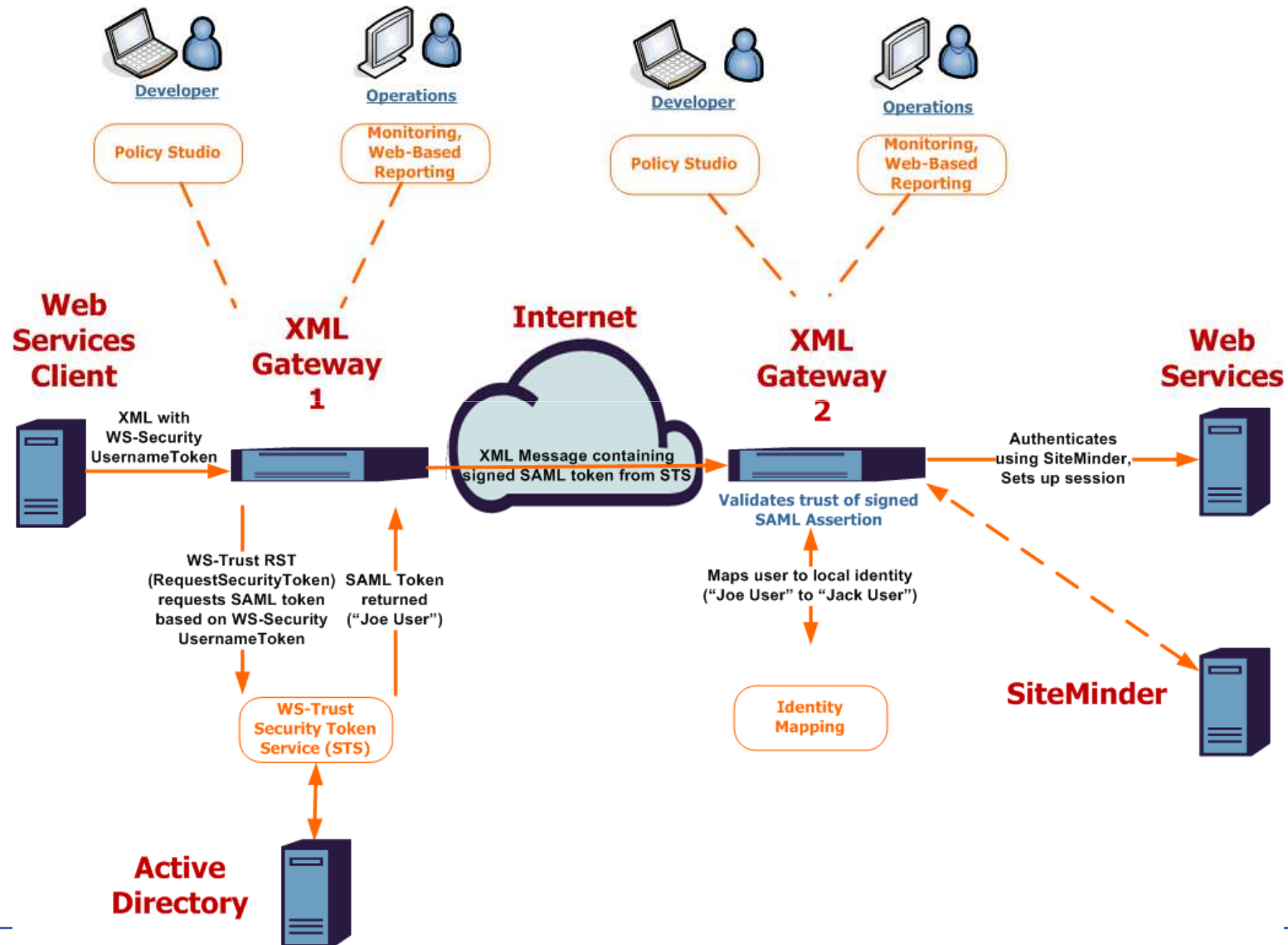
IMPLEMENTAÇÃO: DESREGULAMENTAÇÃO [CANADÁ]



Grande companhia de telefonia móvel italiana

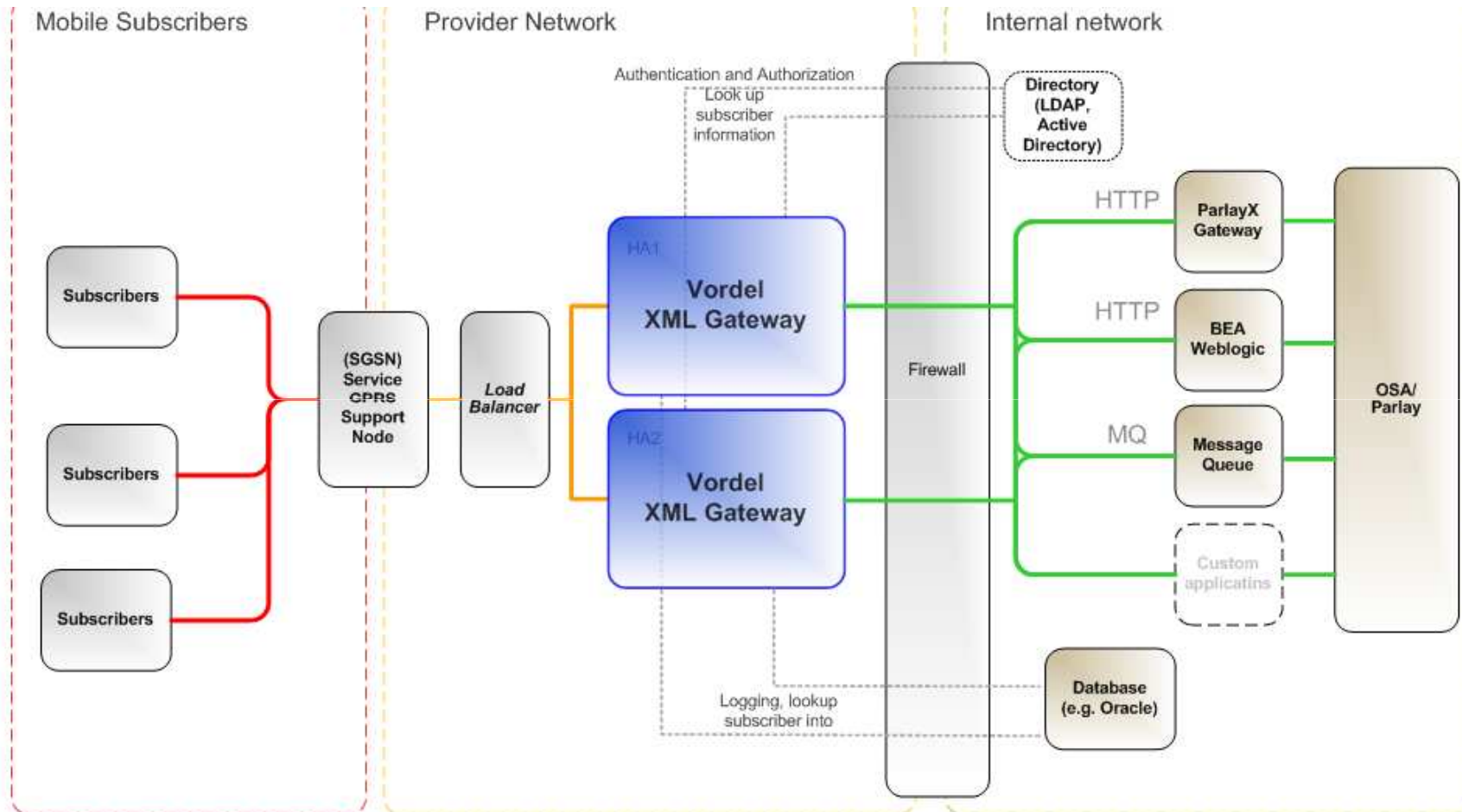
- Testando serviços IPTV. Mensagens XML são utilizadas para solicitar programas e clipes IPTV.
- XML Gateways processam as mensagens XML na entrada que contêm detalhes de cartão de crédito, códigos de marketing (para parceiros), e detalhes dos programas de TV solicitados.
- O XML Gateway permite que as informações de cartão de crédito sejam *encriptadas seletivamente* utilizando a Encriptação XML.
- Dados XML são validados contra Schemas e verificados contra ameaças.
- Integração ao CA SiteMinder garante que todo tráfego é autenticado e autorizado

- SiteMinder é utilizado para toda autenticação e autorização no lado da operadora
- No lado do cliente, geralmente não há SiteMinder. Mas geralmente existe um diretório como Active Directory
- O cliente decidiu utilizar um Serviço de Token de Segurança (STS) para gerar tokens SAML no lado do cliente, e estes são passados para o XML Gateway no lado da operadora.
- Isto permite que ocorra a *Federação de Identidade*. O mesmo usuário final pode ter uma identidade diferente no lado da operadora, comparado com sua identidade no lado do cliente. Isto exige que o XML Gateway faça um *mapeamento de identidade*.
- No lado da operadora, o usuário é identificado em uma sessão do SiteMinder, baseado em sua identidade na operadora.



- ✓ O XML Gateway pode ser colocado na mesma rede que os servidores de aplicação fornecendo os serviços
- ✓ Estes se localizariam atrás do SGSN, que é o gateway para a rede IP
- ✓ O SGSN faz a mediação do acesso à rede em nome de assinantes de serviço móvel e implementa a política de agendamento de pacotes entre diferentes classes QoS. É responsável pelo estabelecimento do contexto de Packet Data Protocol (PDP) com o GGSN (gateway GPRS support node) na ativação

DIAGRAMA DE IMPLANTAÇÃO



Copyright © Vordel 2008

1. Ambiente:

- ✓ **Sistema Operacional:** Red Hat Enterprise Linux ES release 4 (Nahant Update 6)
- ✓ **Servidor:** DELL PowerEdge 1950 - Intel(R) Xeon(R) CPU E5410 @ 2.33GHz, 16GB
- ✓ **Ferramenta de testes:** SOAPui
- ✓ **Versão do XML Gateway:** 5.1.3

2. Teste:

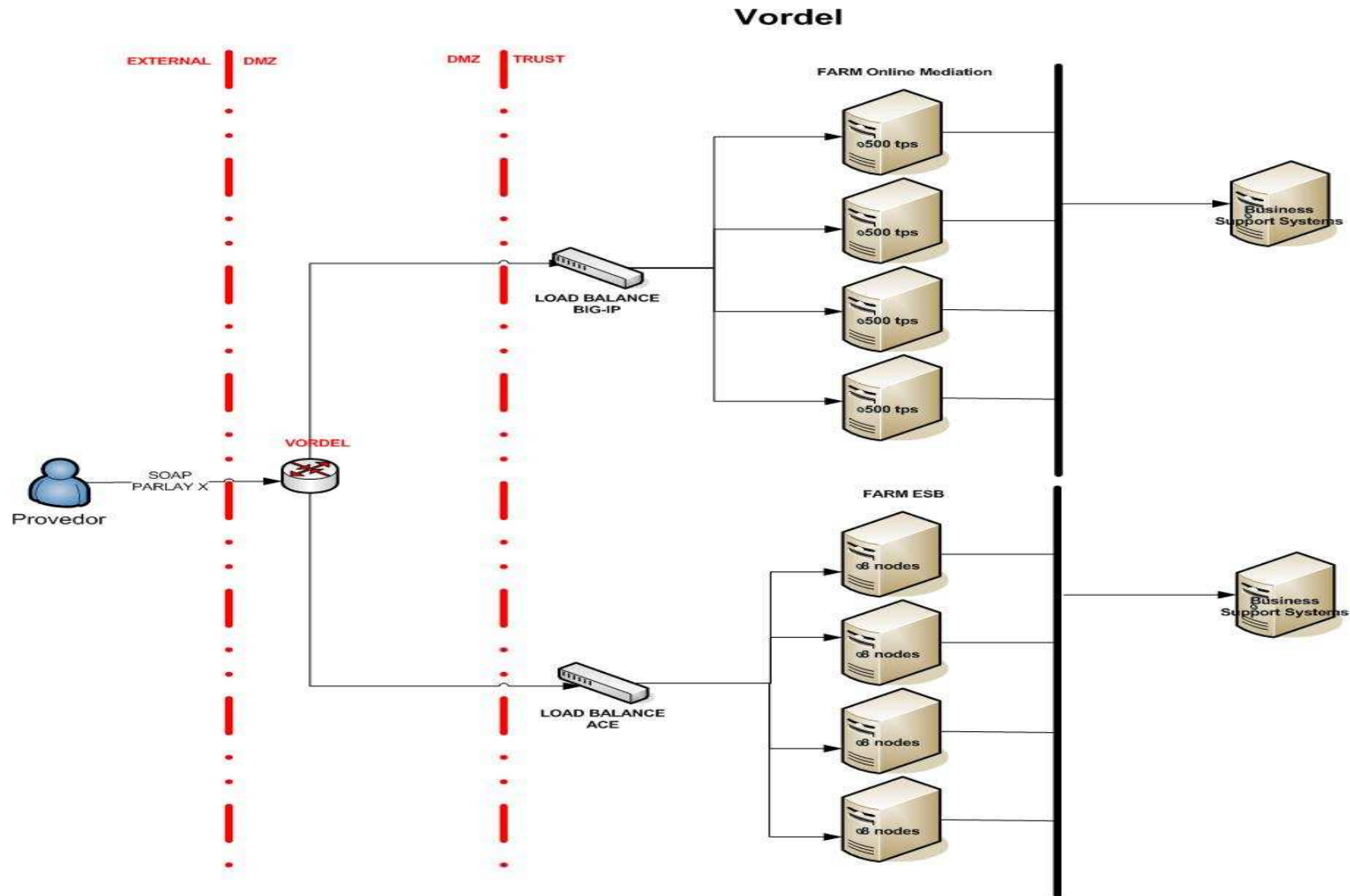
- ✓ Foi selecionado o serviço SiebelGetPositionByUser.
 - ✓ As políticas de teste foram automaticamente criadas no Vordel XML Gateway, a partir da importação do WSDL que define este serviço.
 - ✓ As políticas foram então ajustadas para o ambiente
 - ✓ Os testes foram feitos enviando mensagens XML padrão através do SOAPui para o serviço e comparando os tempos de resposta entre o ambiente atual e o ambiente utilizando o Vordel XML Gateway
 - ✓ Foram feitos testes com novas funções, como Schema Validation
 - ✓ Também foi testado um request ao XML Gateway sem passar para o ESB ou WLI, indicando precisamente o tempo que a mensagem leva “dentro” do gateway
-

	Average response time (ms)	Transactions per second
ANTES		
SOAPUI -> ESB -> WebLogic	2121.15	2.44
SOAPUI -> WebLogic	2309.02	2.64
SOAPUI -> Vordel (XSD) -> WebLogic	1995.87	2.51
SOAPUI -> Vordel -> WebLogic	1895.34	2.64
DEPOIS		
SOAPUI -> Vordel (XSD)	12.77	391.45
SOAPUI -> Vordel	3.46	1443.96

- ✓ De acordo com os testes executados, nas configurações utilizadas, e sem utilizar funções avançadas do Vordel, não é recomendada a sua utilização em conjunto com o ESB, visto que seu desempenho sozinho apresenta-se melhor.
 - ✓ Porém, ao incluir funções avançadas como *Schema Validation*, o ganho em desempenho é flagrante.
 - ✓ A função de *Schema Validation* é uma das que mais demandam processamento do servidor.
 - ✓ Nos dois últimos cenários de teste podemos verificar o poder de processamento e aceleração do Vordel XML Gateway, uma vez que sem a comunicação com o ESB ou WLI o ganho ultrapassa 15.000% (quinze mil por cento).
 - ✓ Todos os resultados foram obtidos sem nenhum *tuning* do servidor, atividade que sempre é executada quando da instalação de um ambiente de desenvolvimento ou produção.
-

- ✓ O cliente pretende utilizar o Vordel para:
 - ✓ Validar cada provedor que trabalhar com eles,
 - ✓ Definir SLA's;
 - ✓ Definir regras
 - ✓ Ter registros confiáveis de auditoria;
 - ✓ Seguir padrões de segurança
 - ✓ Utilizar para federação de identidade.
-

ESTUDIO 7: VAS



Organizações que querem usar Cloud para reduzir custos de fazer negócios

- Aplicações SaaS applications como o Google Mail
- Armazenamento usando Amazon S3
- Automação da força de vendas com Salesforce.com

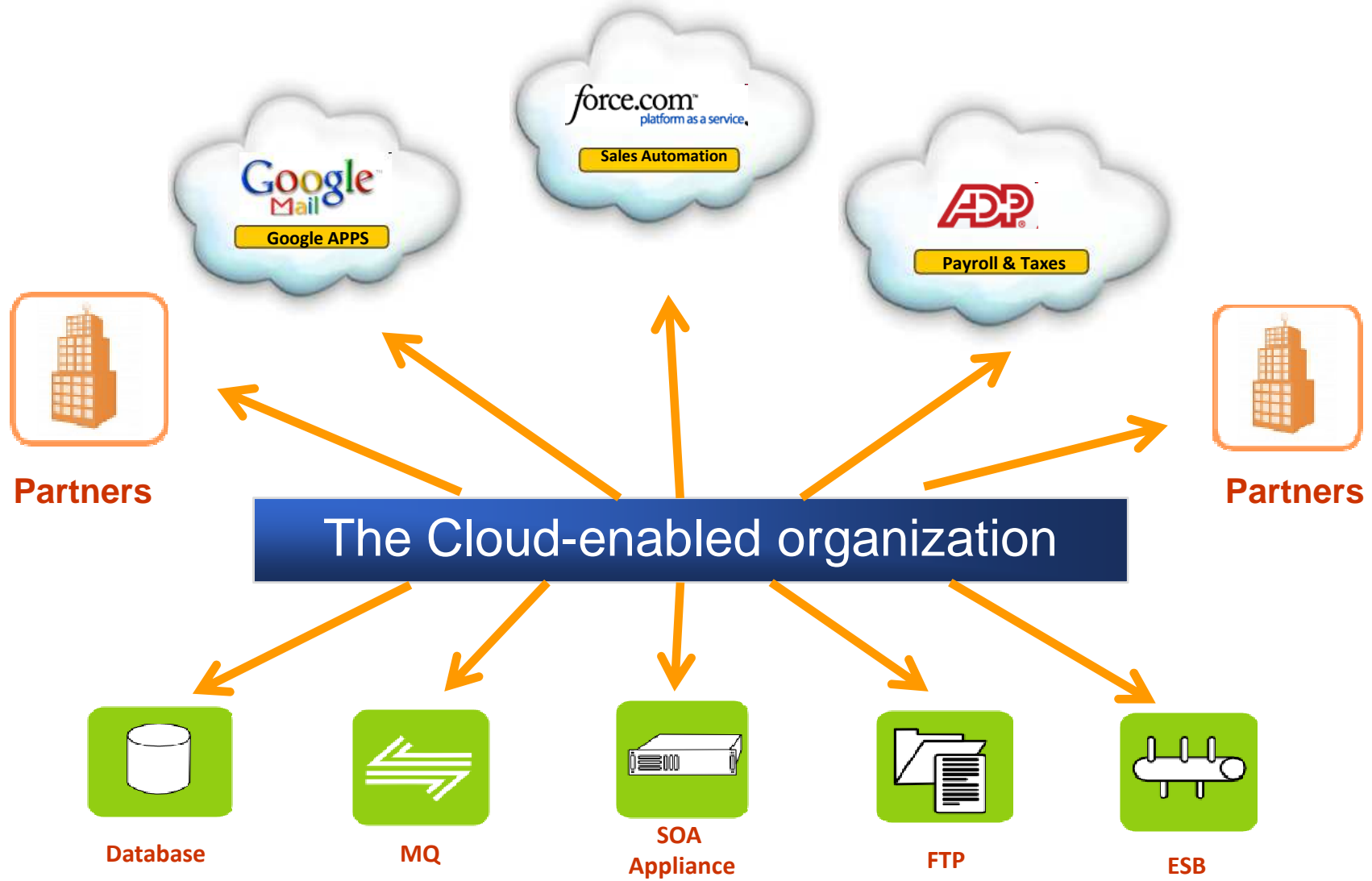


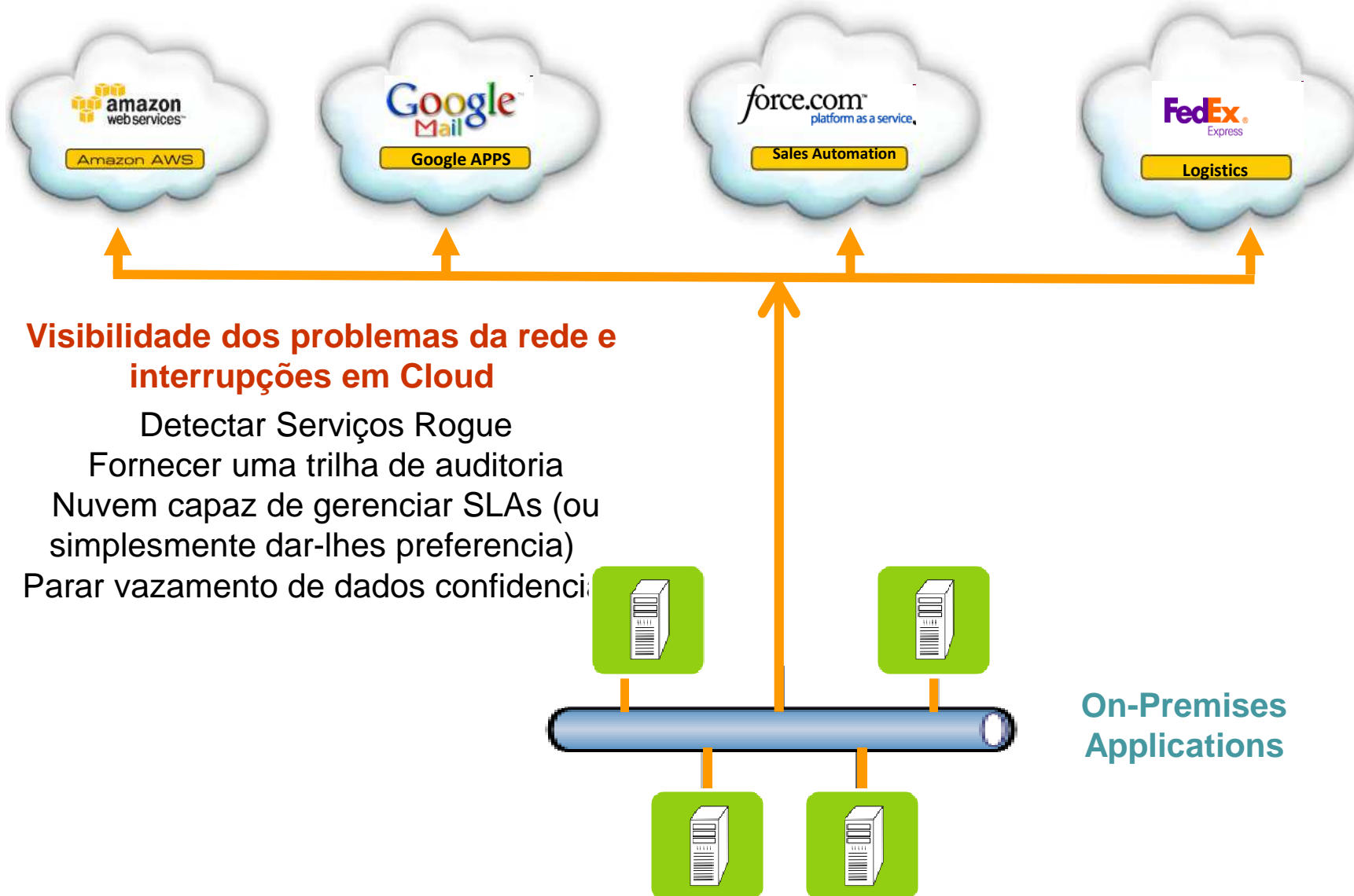
As organizações continuam também em infra-estrutura no local

Bases de dados, filas de mensagens, FTP, aparelhos SOA, transferência gerenciada de arquivos e ESBs



Além disso as organizações se conectam a parceiros para B2B





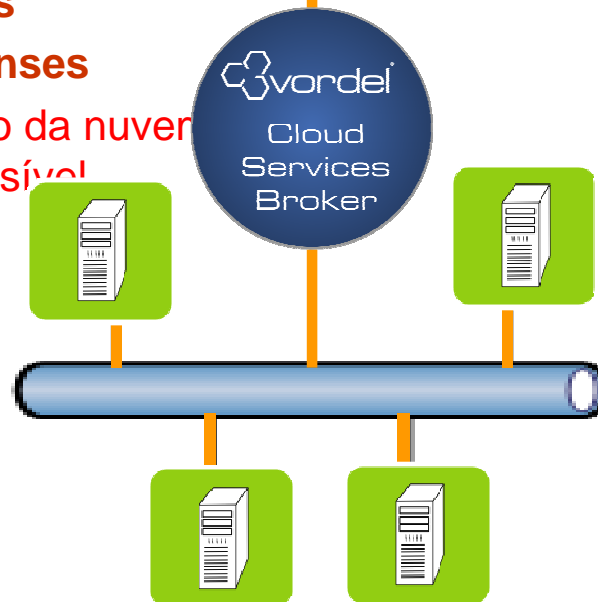
Visibilidade dos problemas da rede e interrupções em Cloud

- Detectar Serviços Rogue
- Fornecer uma trilha de auditoria
- Nuvem capaz de gerenciar SLAs (ou simplesmente dar-lhes preferencia)
- Parar vazamento de dados confidenciais



- **Monitoração do Response Times da Cloud**
- **Detecção de “rogue” services**
- **Caching de requests e responses**

Registros independentes do uso da nuvem
Filtragem de tráfego sensível



Opções de Sistemas Operacionais:

- Incorpora o engine VXA (Vordel XML Acceleration).
- Funciona com os seguintes sistemas operacionais: Windows 7, Vista, XP e Server 2003, Red Hat Linux, Suse Linux ES, Ubuntu Linux, Debian Linux, Solaris 10 Sparc

Opções de Hardware :

- Hardened Appliance
- Software for Windows, Linux, Solaris
- VMware Appliance
- Amazon EC2 Cloud AMI Image

Categoria	Produto
Gerenciamento de Identidade	Oracle Access Manager / CA Siteminder / Tivoli Access Manager Sun Java System Access Manager / RSA Access Manager / Entrust GetAccess
Directory Services	Oracle OID / Sun Directory Server / Active Directory / Novell eDirectory
Servidores de Aplicação	Oracle WebLogic / IBM WebSphere / Microsoft IIS
Integração de Dados	Contivo
Mensageria	Oracle Advanced Queuing / IBM WebSphere MQ / Fiorano ESB / JBOSS Messaging Server / Sonic MQ / TIBCO EMS / TIBCO Rendezvous
Anti-Virus	Sophos / ClamAV
Registros	Oracle Service Registry / HP Systinet
Frameworks	.NET 3.0 & 3.5 / Java / Sun Metro / Apache Axis
Serviços Cloud	Amazon SQS & SDB / Google / Salesforce
Gerenciamento Enterprise	Oracle Enterprise Manager / HP OpenView

	Vordel (all products)	B	C (XML Gateway)	D (XML Gateway)	E	F
Access Control using WS-Security	YES	NO (uses Forum XWall which has no support for WS-Security)	YES	YES	Partial support (Sentry has Access Control support. XWall has no support for WS-Security)	YES
XML Threat Analysis	YES	YES (through Forum XWall software)	YES	YES	YES	YES
Hardware Acceleration	YES (inbuilt in VS3000 appliance, or via third-party acceleration cards in VordelSecure and VordelDirector)	YES	Partial support (through nCipher and Tarari at additional cost; basic system has no acceleration)	YES	Partial support (XWall has is a pure software product. Sentry includes a SSL accelerator)	NO (Software product only, is part of Intel's software group)
Full-featured Web-base Reporting	YES (HTML reporting, Service Level Agreements, monitoring, reporting)	NO	NO	NO	NO	NO
Integration with Identity Management	YES (RSA, Entrust IBM Tivoli, LDAP, SAML, Sun, Oblix/Oracle, etc)	NO	YES	YES	Partial support (Not the same breath of connectors as Vordel has)	NO
Security Token Service	YES	NO	NO	NO	NO	NO
Security testing tool	YES (Vordel SOAPbox)	NO	NO	NO	YES (Forum XRay)	NO
Solution to the "Last Mile" problem	YES (security can be deployed at host)	YES	YES	NO (strictly appliance only)	YES	NO

Example Customers



<p>Federal/ Govt.</p>	
<p>Financial</p>	
<p>Telecoms</p>	
<p>Other</p>	