Zabezpečení platformy SOA

Michal Opatřil
Corinex Group

Corinex Group

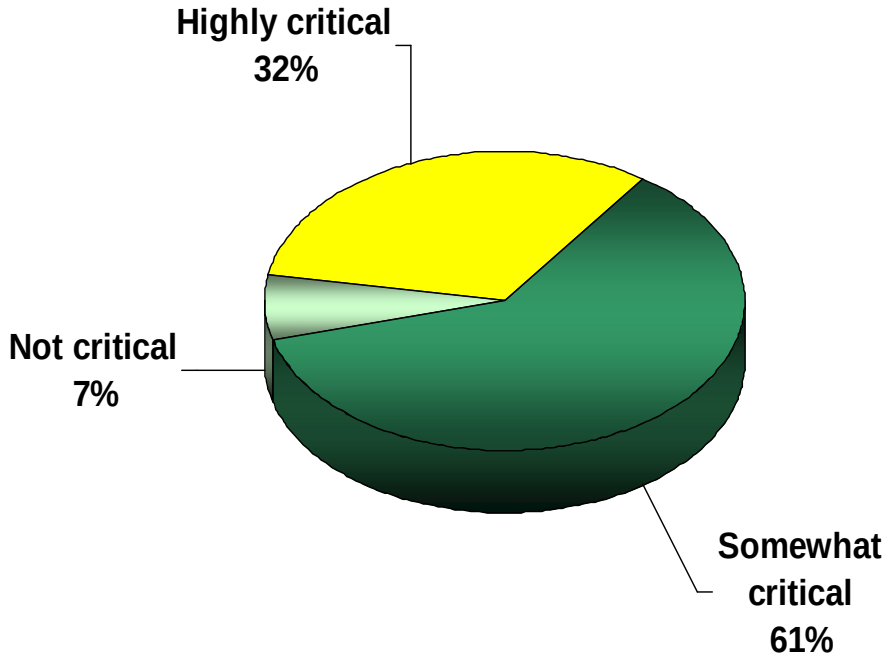
ca Forum | Bratislava 20. október

Corinex Group

- Současný přístup k SOA bezpečnosti
- Požadavky zákazníků
- CA SOA Security Manager
  - Architektura
  - Klíčové vlastnosti
- Proč CA SOA Security Manager

Integrace bezpečnostního řešení SOA s IAM je kritická

Corinex Group



The vast majority of organizations believe integrating SOA-based/Web services security solutions with IAM is critical.

Sourc: Global report on SOA / Web services security initiatives, GMG Insights, Sept. 2008

Tradiční přístup k zabezpečení SOA

Corinex Group

- Aplikace poskytující webové služby si řeší autentizaci sama
- Organizaci ani nezajímá, že má webové služby
- Pro řadu organizací je řešením SSL (to není řešení)

Požadavky zákazníků

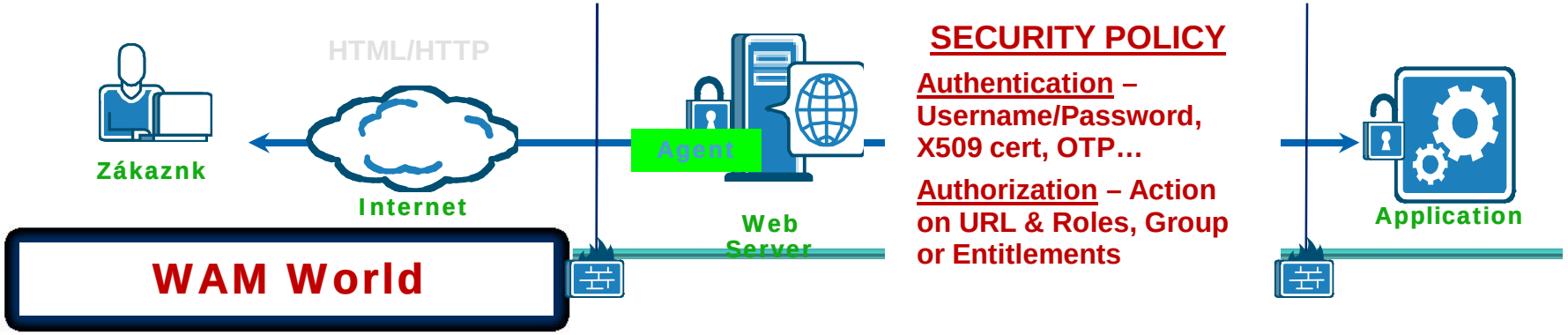
Corinex Group

- Zabezpečit centrální, jednotnou autentizaci webových služeb
- Zabezpečit centrální, jednotnou autorizaci webových služeb
- Autentizace vůči jedné, častěji více aplikacím poskytujícím data
- Zabezpečení různorodých aplikací
- Nezávislost na platformě (.NET, JAVA, Microsoft, Linux/Unix)
- Podpora webových serverů IIS, Apache
- Podpora aplikačních serverů WebSphere, Weblogic, Jboss
- Výkonné a škálovatelné řešení (i miliony identit!)

Zabezpečení webu a webových služeb
Rozdíly a shody

Corinex Group

Webové aplikace: Uživatel, přístup via web browser, přímá interakce s aplikací

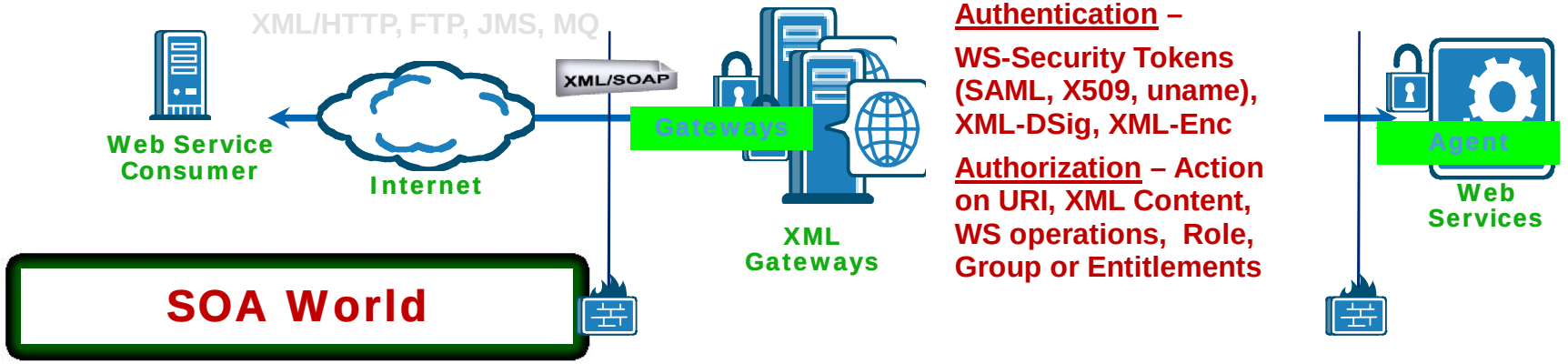


SECURITY POLICY

Authentication – Username/Password, X509 cert, OTP…

Authorization – Action on URL & Roles, Group or Entitlements

Webové služby: Služba/aplikace, velmi často běží v uživatelově kontextu, interakce s webovou službou



SECURITY POLICY

Authentication –

WS-Security Tokens (SAML, X509, uname), XML-DSig, XML-Enc

Authorization – Action on URI, XML Content, WS operations, Role, Group or Entitlements

CA Forum | Bratislava 20. október

CA SOA Security Manager

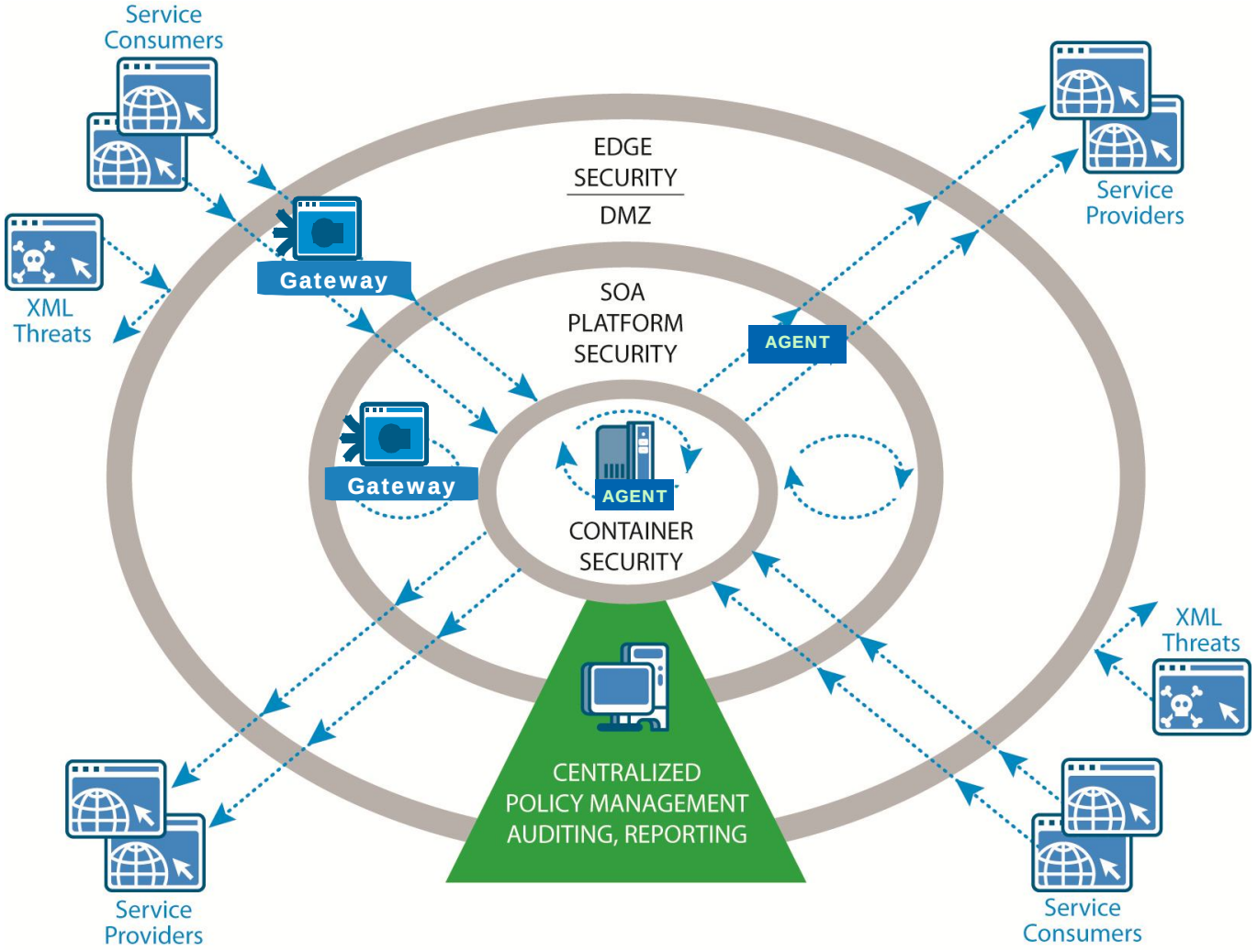
Jak zabezpečit webový business

Corinex Group

> Podpora splnění požadavků na zabezepčení, soulad s předpisy pro webové transakce
> Redukce nákladů díky znovu použití kódu, automatizaci a centrální správě
> Snížení rizik prostřednictvím konzistentních přístuových politik
> Zjednodušení přístupu pro uživatele

CA SOA Security Manager

Corinex Group



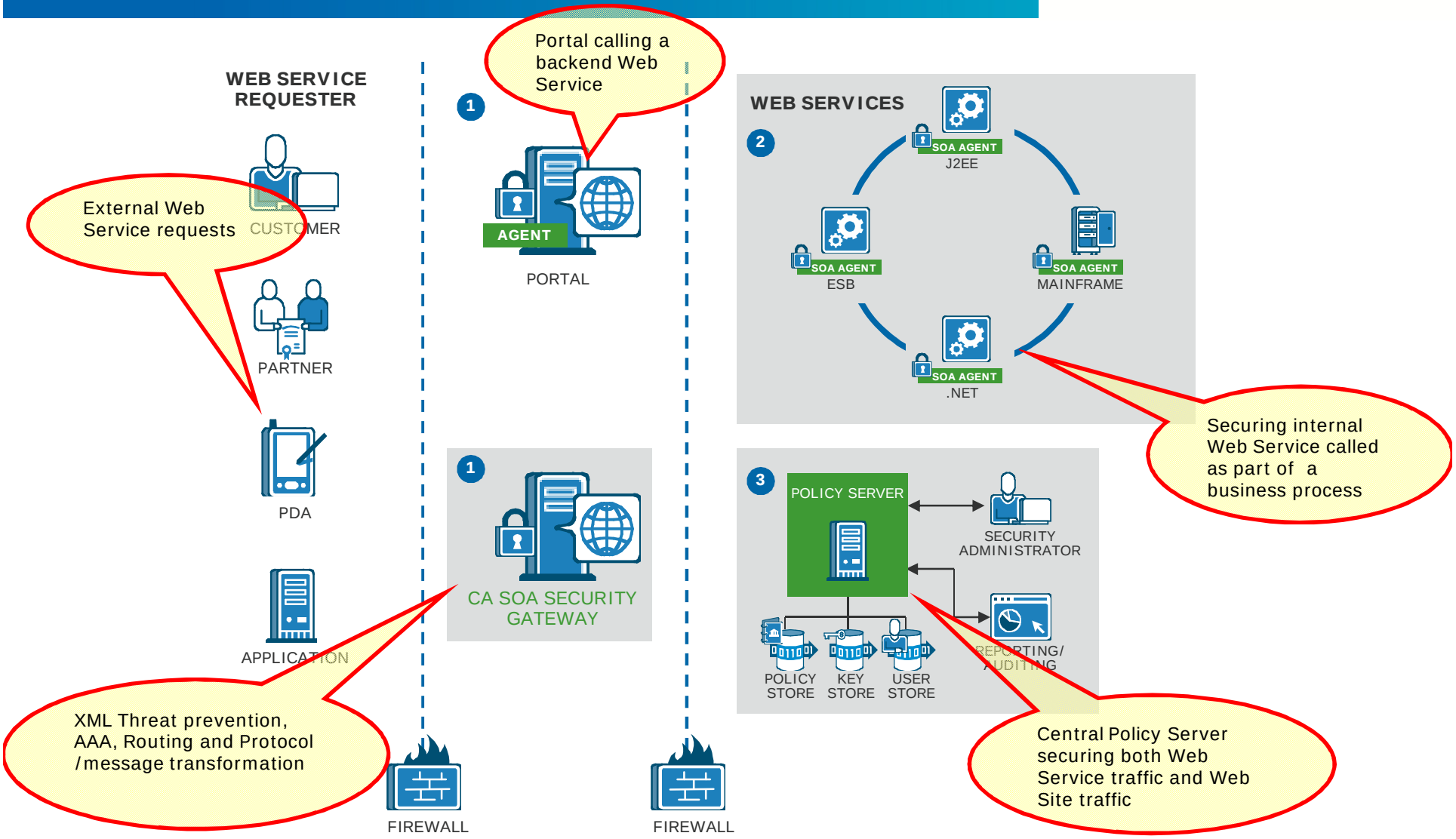
CA SOA Security Manager
Klíčové komponenty

Corinex Group

- Centrální Policy Server
  - Jedno místo pro řízení přístupů, politik a auditu
- SOA Security Gateway
  - Proxy-based nasazení & XML anti-threat služby
    - Perimeter-based AAA (autentizace, autorizace, accounting)
    - Denial of Service, SQL injection, XML schema validation
    - Routing, SLA monitoring
- SOA Agent for web service containers
  - Bezpečnost poslední míle – zabezpečení v místě webových služeb
  - Rošiřuje možnosti AAA k webovým služebám běžících jako J2EE kontejnery (IBM WebSphere, Oracle WebLogic and RedHat JBoss)
  - Podpora web serverů IIS, IHS, Apache, SunOne
- SOA Security Manager SDK for custom SOA Agents

CA SOA Security Manager
Referenční architektura

Corinex Group



CA Forum | Bratislava 20. október

Referenční architektura

Corinex Group

— SOA Security Manager
  – Gateway má SOA agenta embedded

Edge Gateways

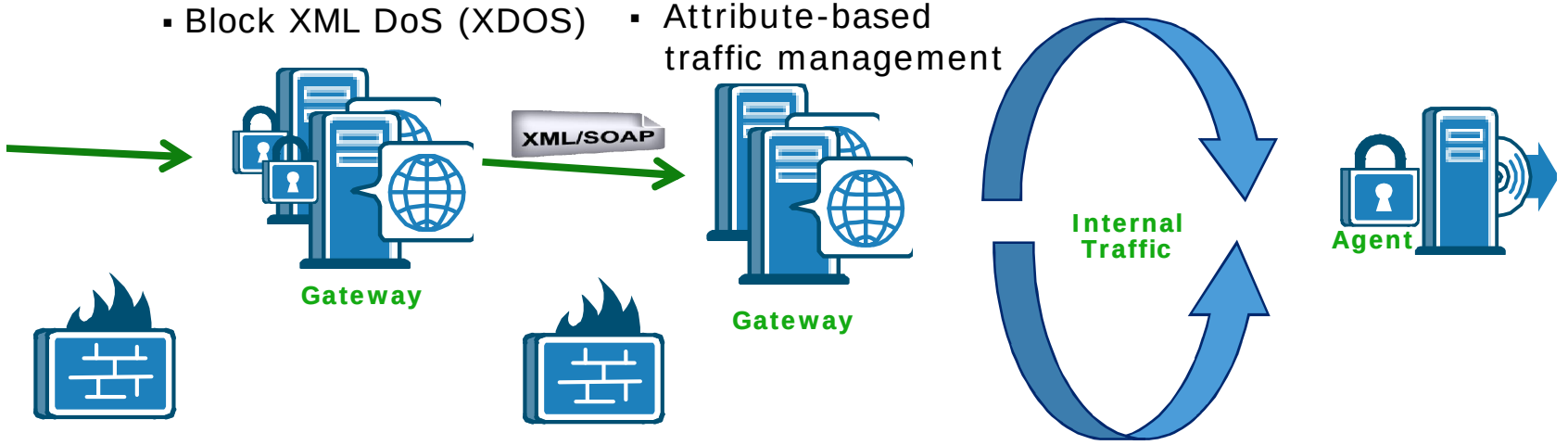
- Service Virtualization
- Identity based security
- Injects attributes into messages
- Throttling, rate-limiting
- XML Threat Scanning
- Block XML DoS (XDOS)

Internal Gateways

- Protocol Mediation (HTTP to JMS, FTP, etc)
- XML Processing Offload
- Transformation (XSLT, etc)
- SLA monitoring
- Attribute-based traffic management

Endpoint Agents

- Identity based Last-mile security
- Dynamic Fine-grained authorization at the content and web service operation



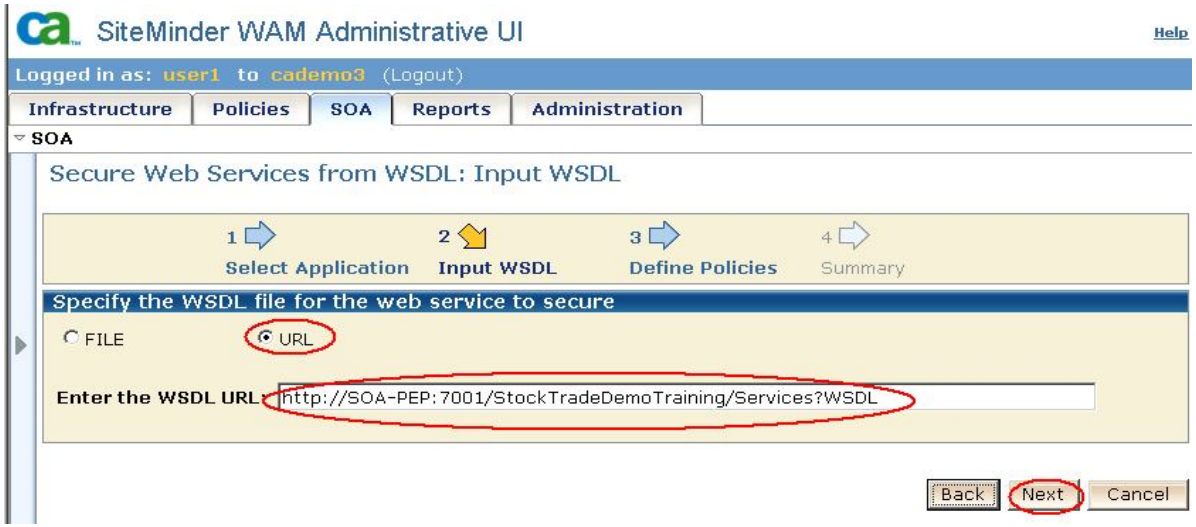
CA SOA Security Manager
Klíčové vlastnosti

Corinex Group

- Autentizace na základě obsahu
  - WS-Security – Username, X509, SAML (XML Encryption/Signing)
  - XML Document Credentials Collector (DCC)
  - XML Digital Signature
  - SAML Session Ticket
- Model dynamické autorizace
  - Autorizace na základě XML proměných vyhodnocovaných dle politiky
- XML Threat prevention, routing, transformation, SLA monitoring
- Session synchronizace
  - Single sign-on přes více webových služeb
- Credential mapping
  - WS-Security header generation
  - SAML Session ticket generation

SOA/Web Service GUI

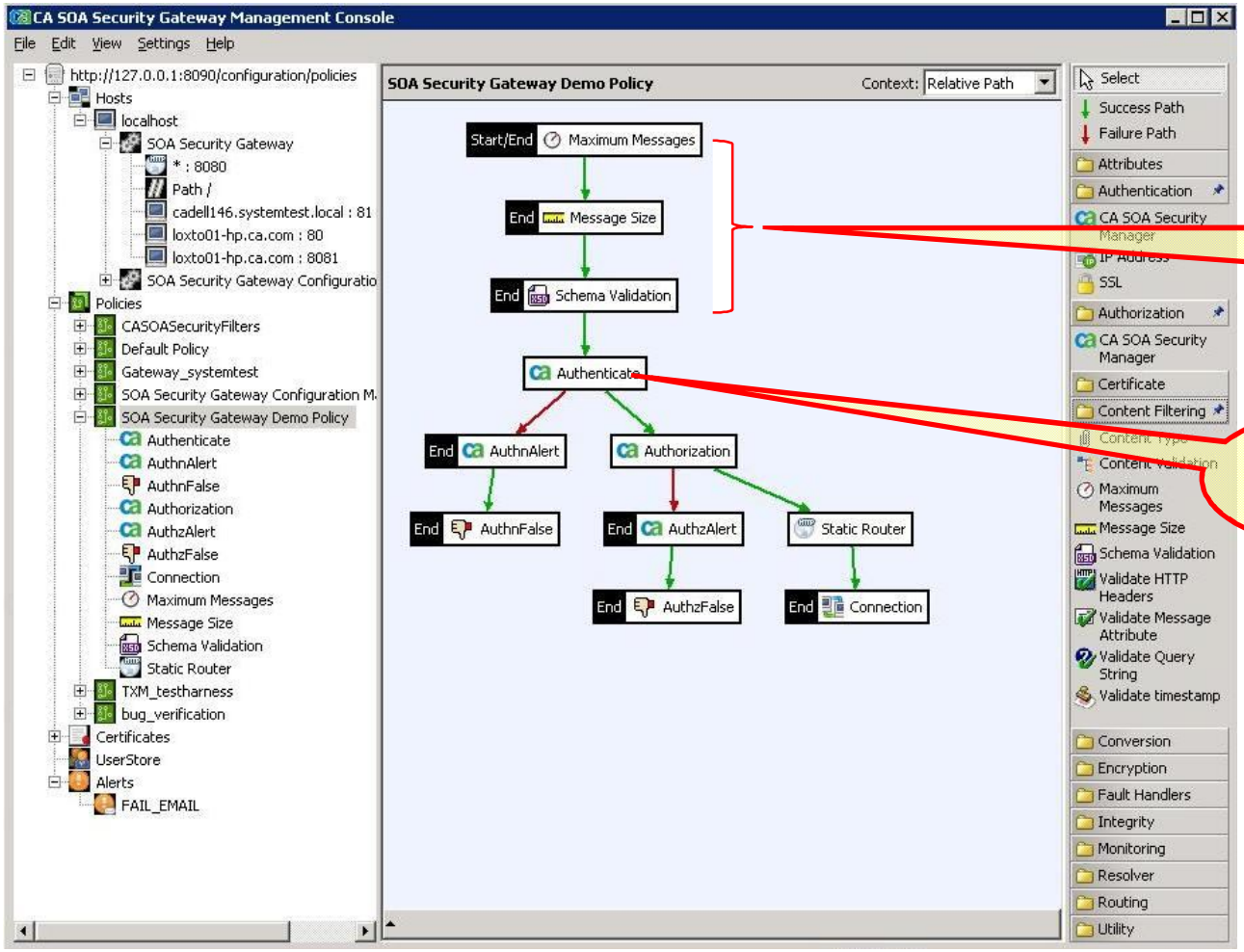
Corinex Group



- Podpora WSDL pro vytváření bezpečnostních politik
- Jedno UI ke správě bezpečnosti webu a webových služeb
- Postaveno na CA SiteMinder WAM UI
- Využívá a povyšuje SiteMinder WAM Administrative Model

CA SOA Security Manager
Gateway Policy

Corinex Group

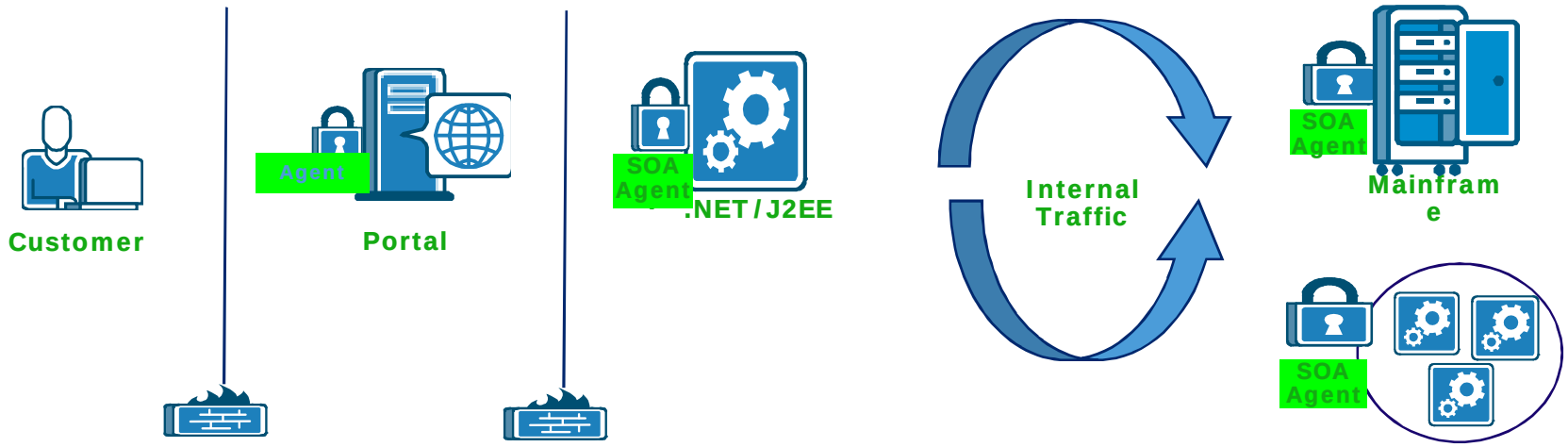


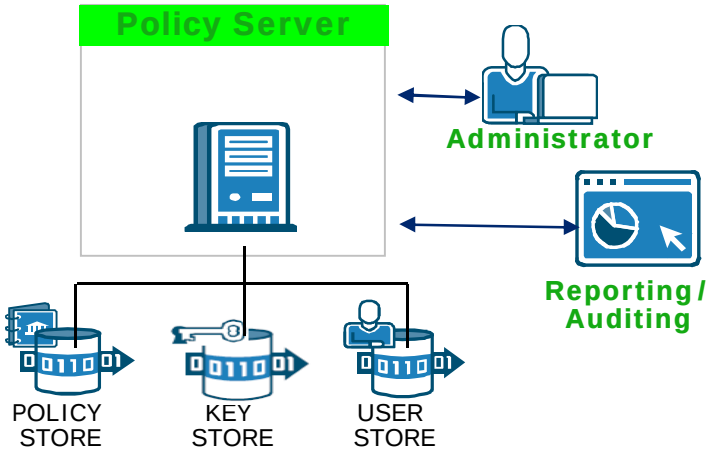
XML threat prevention policies

Identity based Authentication and Authorization

CA SOA Security Manager

Use Case - *Portál přistupuje k Back-end webovým službám SSO*

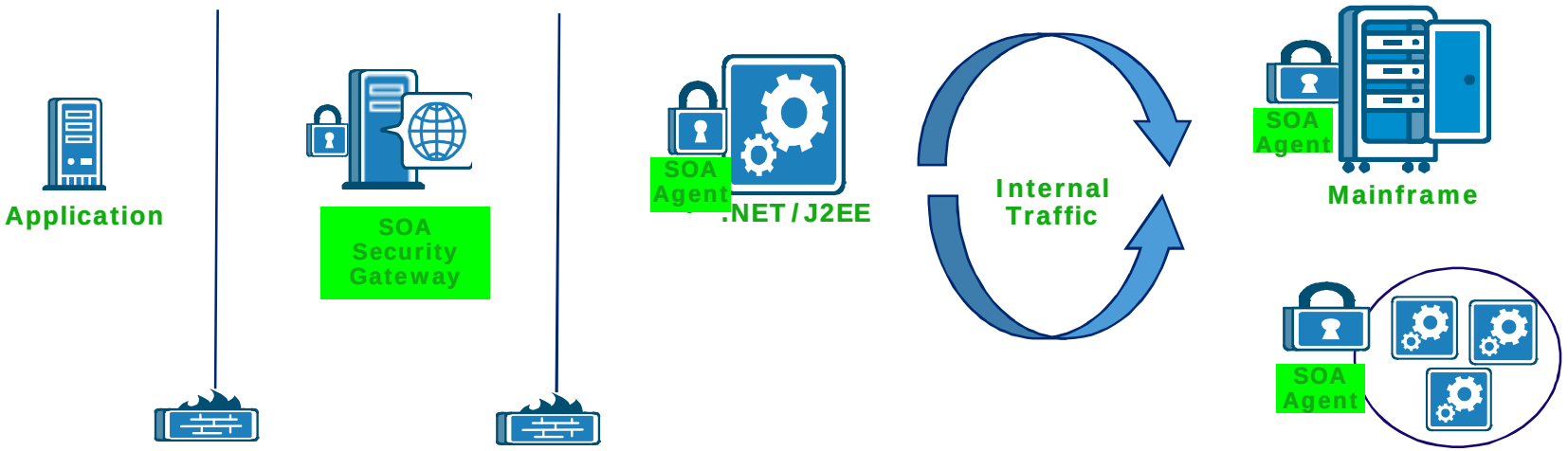




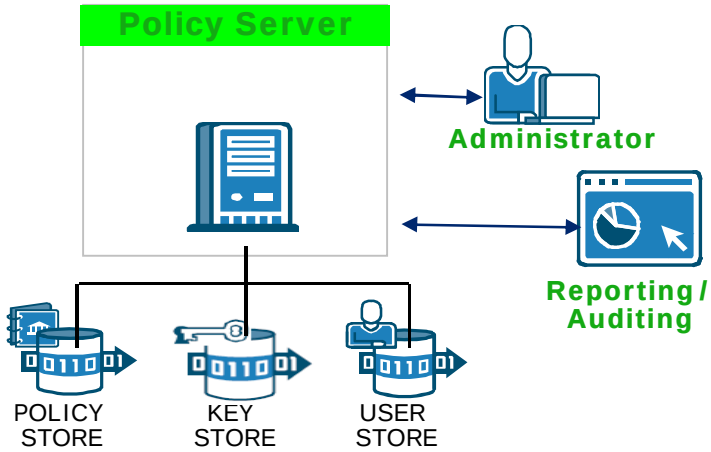
- Single-Sign-on procházející portálem a současně použitá i pro webové služby volané portálem
- Centrální policy server pro WAM I webové služby
- Centrální audit a reporting

CA SOA Security Manager

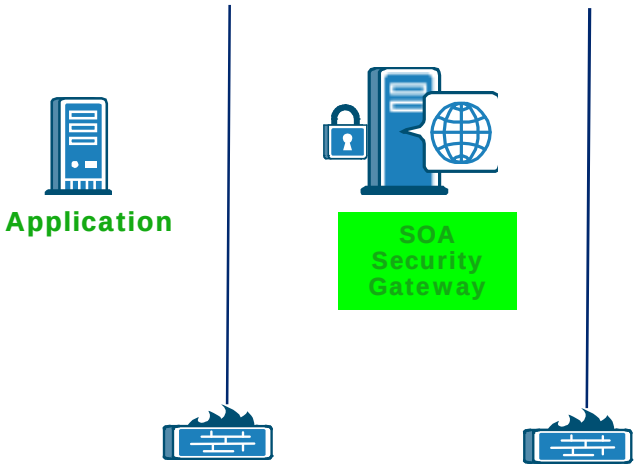
Use Case – Zabezpečení webových služeb od aplikace až ke zdroji



- Bezpečnost je vynucována na každé úrovni
- SSO je poskytováno pro webové služby
- Centrální bezpečnostní policy management
- Centrální audit a reporting

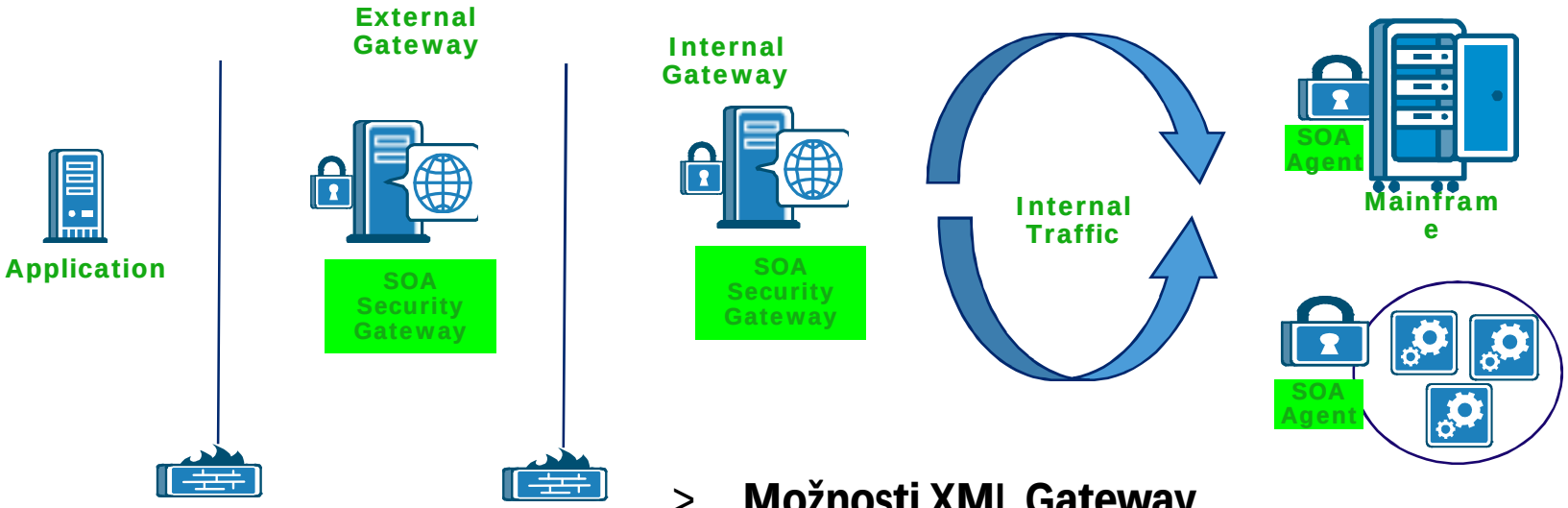


CA SOA Security Manager
Use Case – *XML Threat Prevention*



- **XML Threat prevention**
  - XML Schema validace
  - Prevence DoS
  - Prevence SQL a XPath injections
  - Kontrola velikosti zprávy
  - Kontrola atributů zrpávy HTTP hlavičky
  - Ochrana vůči replay útokům
  - Validace obsahu XML před validací schématu
  - Odstranění příloh
  - Kontrola IP adres klienta

CA SOA Security Manager
Use Case – *Routing a protokol transformace*



- **Možnosti XML Gateway**
  - Překlad protokolů HTTP ⇔ JMS
  - XSLT transformace
  - Message routing na základě obsahu
  - Ovlivnění rychlosti odpvědí
  - SLA Monitoring

CA SOA Security Manager
řízení bezpečnosti SOA

Corinex Group

- Centrální autentizace a autorizace webových služeb
- Integrované řešení s přístupem k webu (SiteMinder)
- Zabezpečení celé cesty od požadavku k poskytovateli
- Autentizace vůči více zdrojům a různým aplikacím
- Nezávislost na platformě (.NET, JAVA, Microsoft, Linux/Unix)
- Podpora webových serverů IIS, Apache
- Podpora aplikačních serverů WebSphere, Weblogic, Jboss
- Výkonné a škálovatelné řešení (i miliony identit!)

Otázky