Secur.Net
Always Online, Always Secure!

Conferência
Segurança em Sistemas de Informação

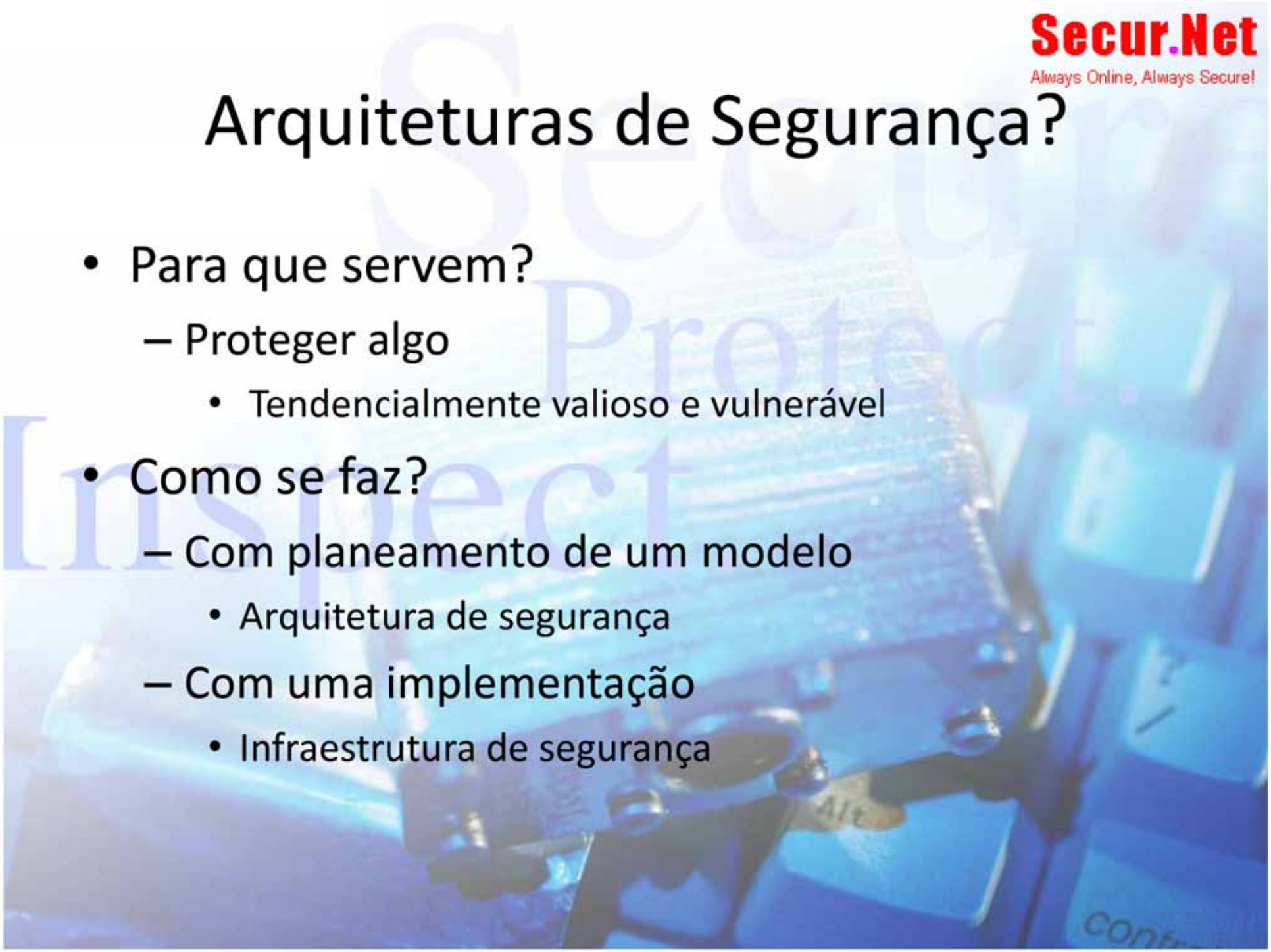
"Arquiteturas Seguras"

Miguel Santiago

Divisão de Segurança da
ReLoad – Consultoria Informática, Lda.

Arquiteturas de Segurança?

- Para que servem?
  - Proteger algo
    - Tendencialmente valioso e vulnerável
- Como se faz?
  - Com planeamento de um modelo
    - Arquitetura de segurança
  - Com uma implementação
    - Infraestrutura de segurança



Arquitetura de Segurança

- Depende da dimensão
- O desenho deve ter como prioridades:
  - Agilidade do negócio
  - Desafios sociais e técnicos
  - Manter a política de segurança
  - Incorporar avanços tecnológicos
- A organização geral deve ter como base a classificação de dados: Pública, Proprietária e Confidencial
- Os procedimento devem seguir standards de referência

Elementos de Arquitetura de segurança

- Política de segurança
- Domínios de segurança (Security Domain)
- Níveis de confiança (Trust Levels)
- Divisão em camadas (Security Layers)

Política de Segurança

- Princípio orientador da segurança dentro da organização
- É o conjunto de documentação composta por:
  - Carta de princípios de segurança
  - Procedimentos de segurança
  - Guias de utilização de recursos
  - Guias de classificação de informação
  - Documentação suporte aos Standards adoptados

Domínios de Segurança

- Domínio do Utilizador
  - Localização do utilizador e tipos de dispositivos
- Domínio de Transporte
  - Redes de dados: locais e remotas
- Domínio de Apresentação
  - Servidores Web, mail, FTP, Voip
- Domínio de Dados
  - Bases de dados, file servers, aplicação

Níveis de Confiança

- Classificação de utilizadores
  - Níveis de acesso á Informação
  - Métodos de autenticação e autorização
  - Risco
- Classificação de redes
  - Nível de segurança do acesso (autenticação, cifra, *compliance*)
  - Níveis de acesso a recursos internos da organização
- Classificação de servidores de apresentação
  - Classificação da informação apresentada
  - Acessibilidade dos mesmos
- Classificação de Armazenamento de dados
  - Níveis de classificação da informação armazenada

Confidencialidade

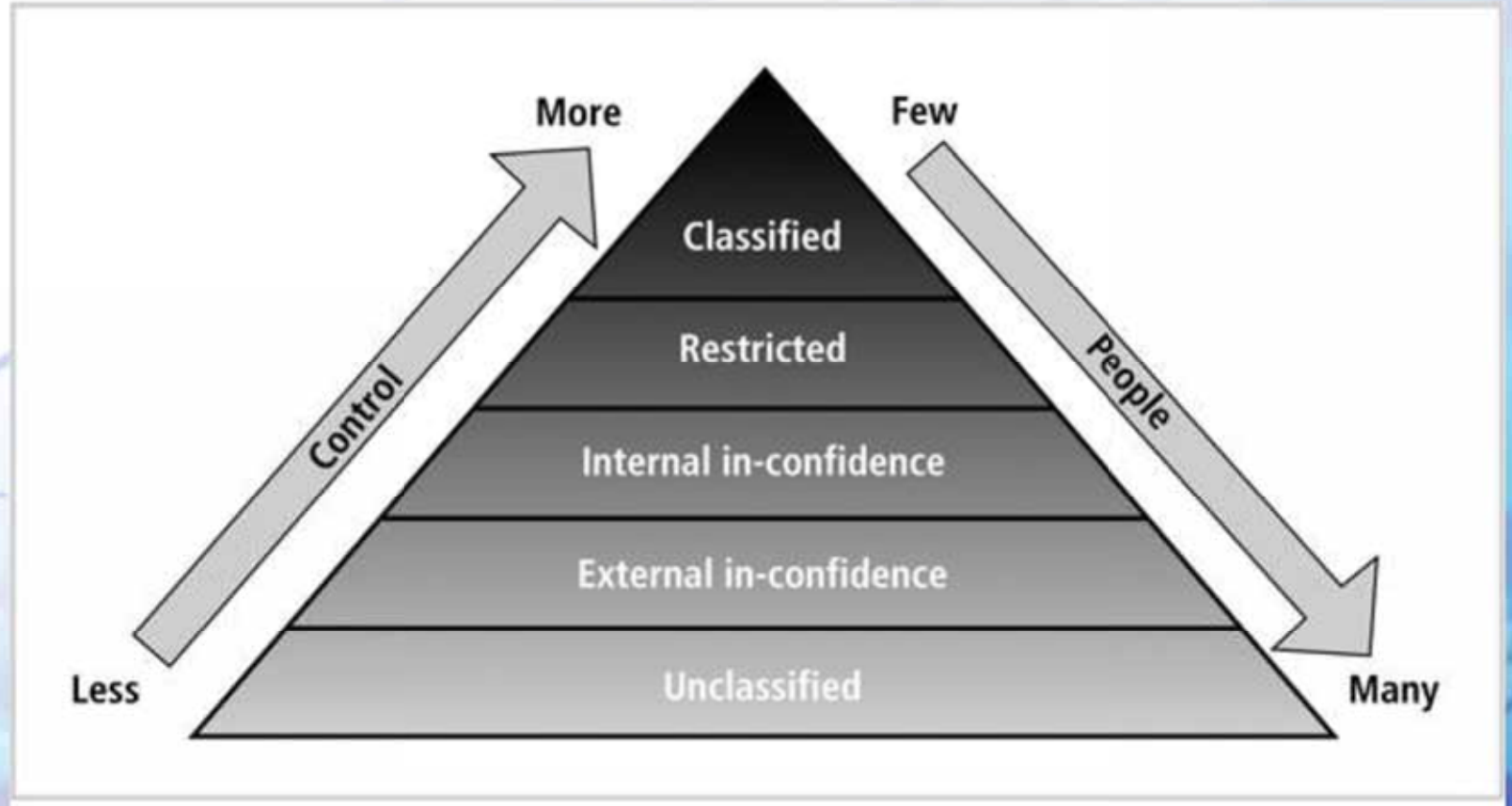


FIGURE 1-6 Confidentiality classification

Divisão em Camadas

- A Divisão em camadas permite:
  - Organizar a informação pela sua classificação
  - Organizar os servidores pela sua classificação
  - Organizar as redes pela sua classificação
  - Organizar os utilizadores e dispositivos pela sua classificação
  - Implementar a política de segurança nos acessos entre as várias camadas
  - Monitorizar atividades entre as camadas
  - Diminuir a superfície de ataque

Secur.Net
Always Online, Always Secure!

Infraestrutura de Segurança

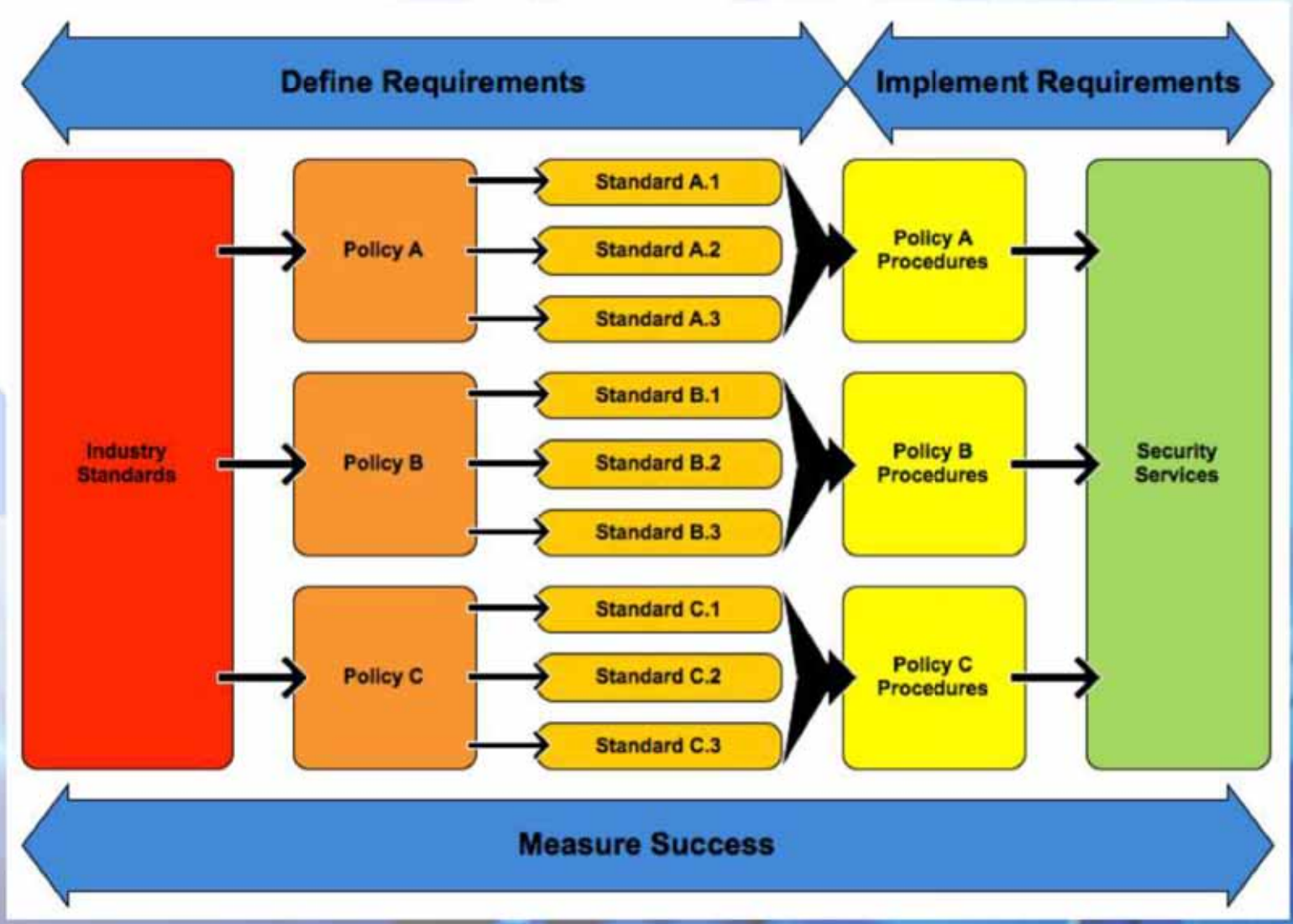
- Documentação
- Serviços de segurança
- Tecnologia

Secur.Net
Always Online, Always Secure!

Documentação

- Políticas
- Standards
  - ISO 27001/27002
  - NIST SP 800-53
  - SOX
  - PCI DSS
- Procedimentos de segurança
- Guias de utilização
- Relatórios e Auditorias

Framework



Secur.Net
Always Online, Always Secure!

Serviços

- Ações de sensibilização dos utilizadores
  - Boas práticas
  - Visibilidade
- Administração da segurança
  - Monitorização
  - Resposta a incidentes
  - Auditorias
- Análise e minimização preventiva do risco

Secur.Net
Always Online, Always Secure!

Exemplos de Políticas

ISO 27001/27002	NIST SP 800-53 Rev 2	SECURITY POLICY
07.01.03, 11.02.03, 11.03.01, 11.03.02, 11.03.03	PL-4, PS-6	**Acceptable Use**
14.01.02, 14.01.03, 14.01.04, 14.01.05	CP-(1-10)	**Business Continuity and Disaster Recovery Plan**
06.01.04, 06.02.03, 12.01, 12.05, 15.01.02	SA-(1,6,9)	**Contract Security for Information**
12.03.01, 12.03.02, 15.01.06	IA-7, SC-(8,9,12,13)	**Cryptographic Controls**
07.02, 07.02.01, 07.02.02, 10.07.03	AC-16, MP-3	**Data Classification**
06, 07.02.02, 09.01, 10, 11, 12, 15	MP-1, SC-(8,9), SI-(1,7)	**Data Protection**
06.01.05, 06.01.06, 13.01.01, 13.01.02, 13.02	IR-(1-7)	**Incident Management**
06.01.01, 06.01.02, 06.01.07, 06.01.08	PL-1	**Information Security Management**
06.02.01, 07.01.03, 08.02.01, 10.02, 10.10.03, 11.01.01, 11.04, 11.05, 11.06.02	AC-(1,2)	**Information System Authorization and Account Management**
06.02.01, 07.01.01, 10.01.03, 10.10.05, 15.02, 15.03	AU-(1-11), RA-(3-5), SA (5,11), CA-(1,2) AC-5, IR-3, CP-4, SI-6	**Information Systems Auditing & Testing**

Secur.Net
Always Online, Always Secure!

Exemplos de Políticas

ISO 27001/27002	NIST SP 800-53 Rev 2	SECURITY POLICY
06.01.03, 10, 11, 12, 15	SC-1, SI-1	**IT Operations Security**
06.01.03, 06.01.05, 08.01, 08.02, 08.03, 13.01, 15.01, 15.02.01	PS-(1-8)	**Personnel Security for Information Systems**
09.01, 09.02, 13.01.02, 14.01.03	PE-(1-17)	**Physical and Environmental Security**
14.01.02, 08.02.02	RA-1	**Risk Management**
10.10.01, 10.10.02, 13.01.01, 13.02.03, 15.01, 15.02.01, 15.02.02	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, RA-1, MA-1, MP-1, IA-1, IR-1, PE-1, PL-1, PS-(1,7), SA-(1,9), SC-1, SI-1	**Security Compliance Management**
05.01.01, 05.01.02	PL-1	**Security Policy Architecture**
05.01.02, 06.02.03, 08.02.02	AT-(1-4)	**Security Training and Awareness**
07.01.02 , 07.02, 07.02.01	Appendix B	**Standardized Glossary - Taxonomy**
10.01.04, 10.03.02, 10.07.04, 12.01.01, 12.04.02, 12.04.03, 12.05.01, 12.05.03	SA-(3,8,11)	**System Development Lifecycle Security**
11.02, 11.04.02, 11.05.02	IA-(1,2)	**User Identification and Authentication**

Secur.Net
Always Online, Always Secure!

Tecnologia

- Firewalls
- IDS
- DLP
- WAF
- DB Firewall
- 802.1x e EndPoint Compliance
- Identity Awareness
- Autenticação Forte e PKI

Casos Práticos - Primórdios

Muralha da China

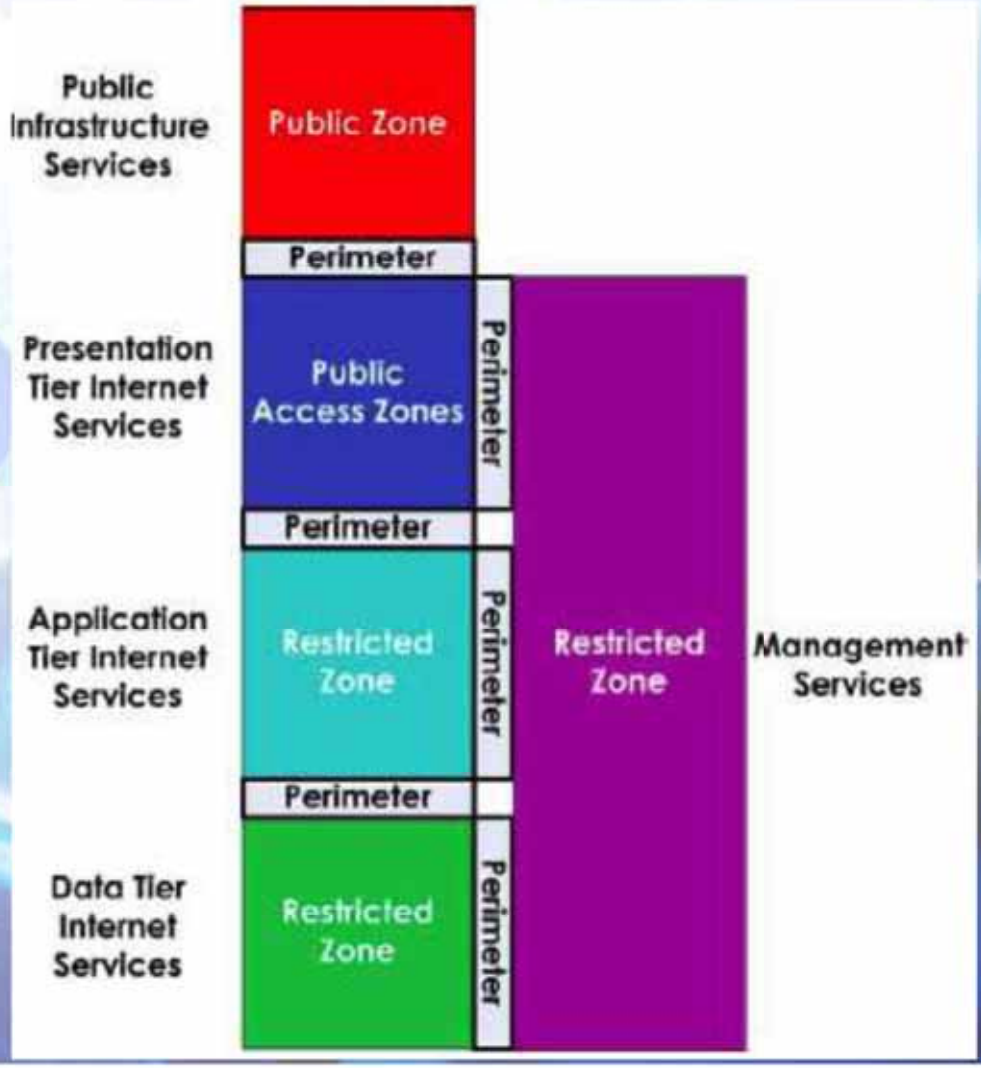
Cidades entre Muralhas

Secur.Net
Always Online, Always Secure!

Defesa Perímetrica

Exemplo Modelo Ref: ITSG-38

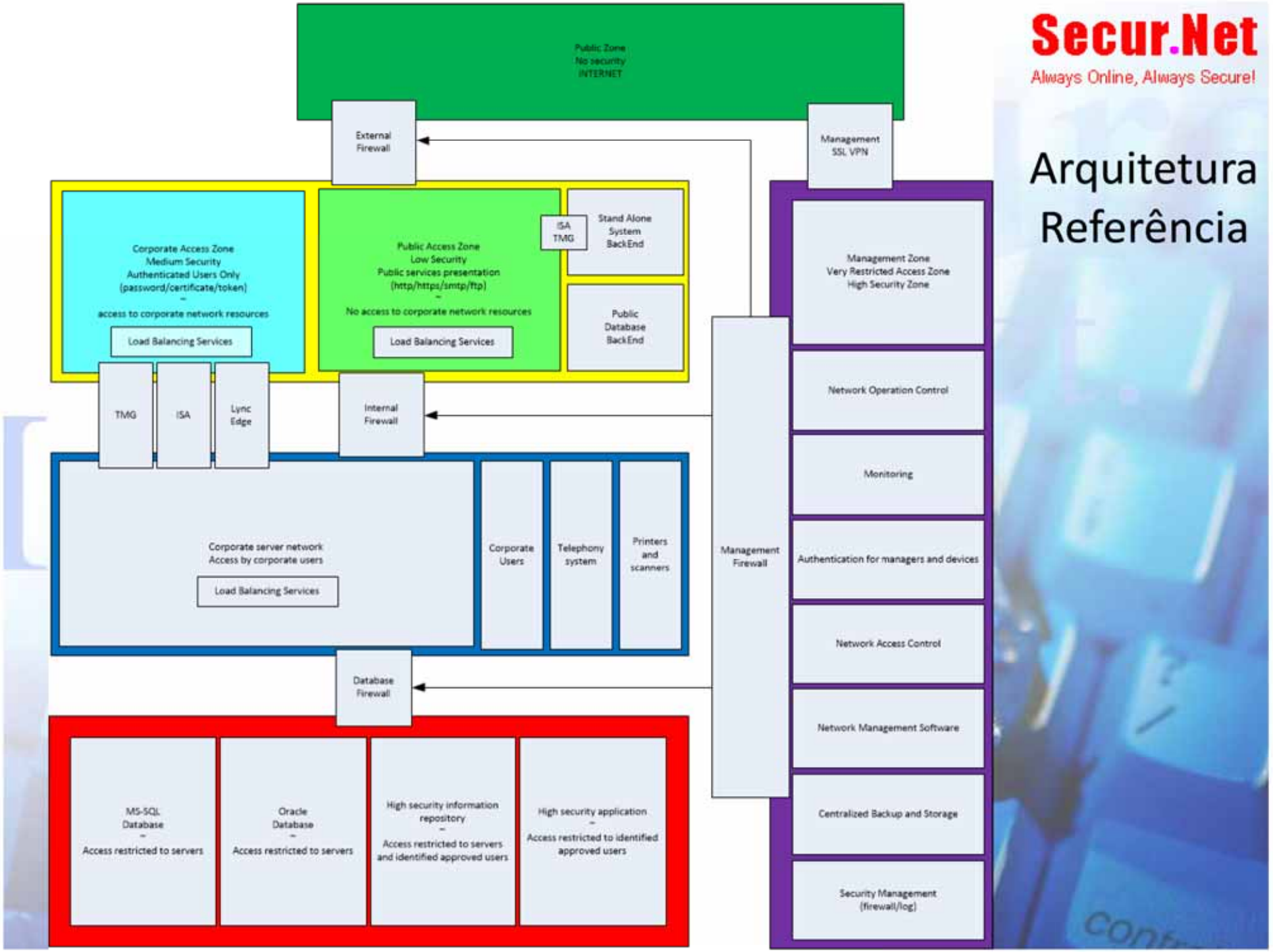
http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg38-eng.html



Secur.Net

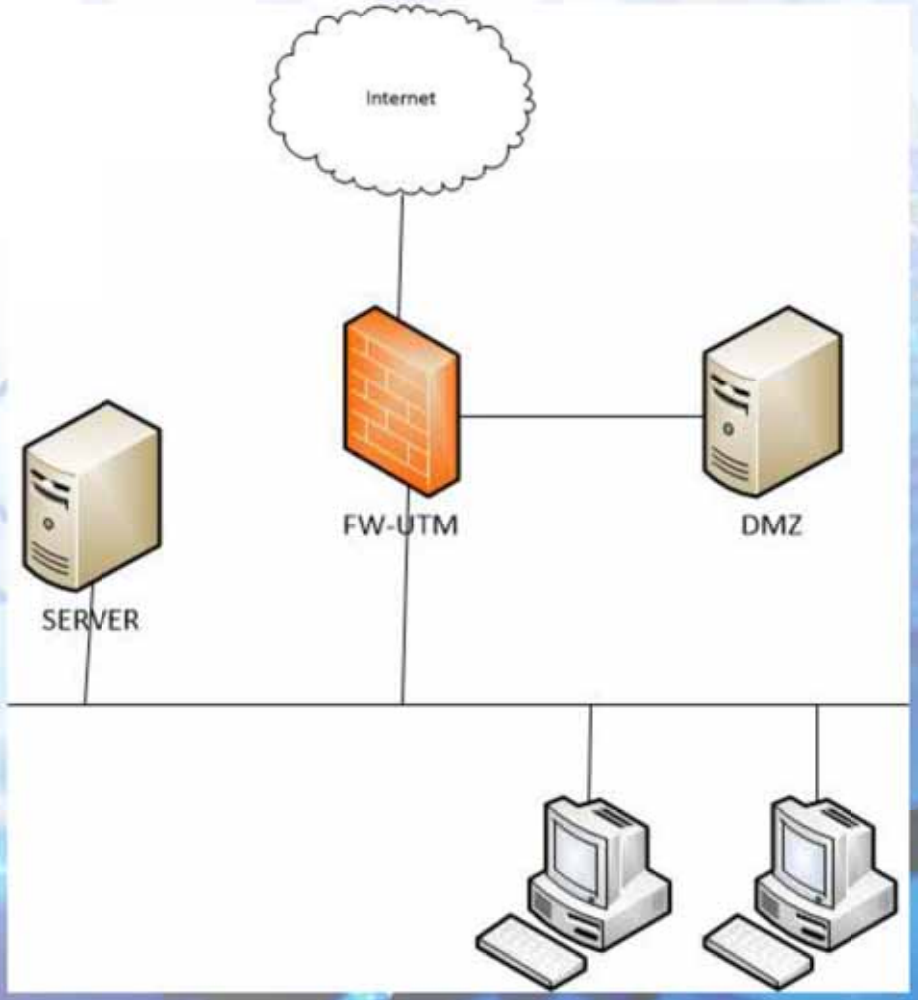
Always Online, Always Secure!

Arquitetura Referência



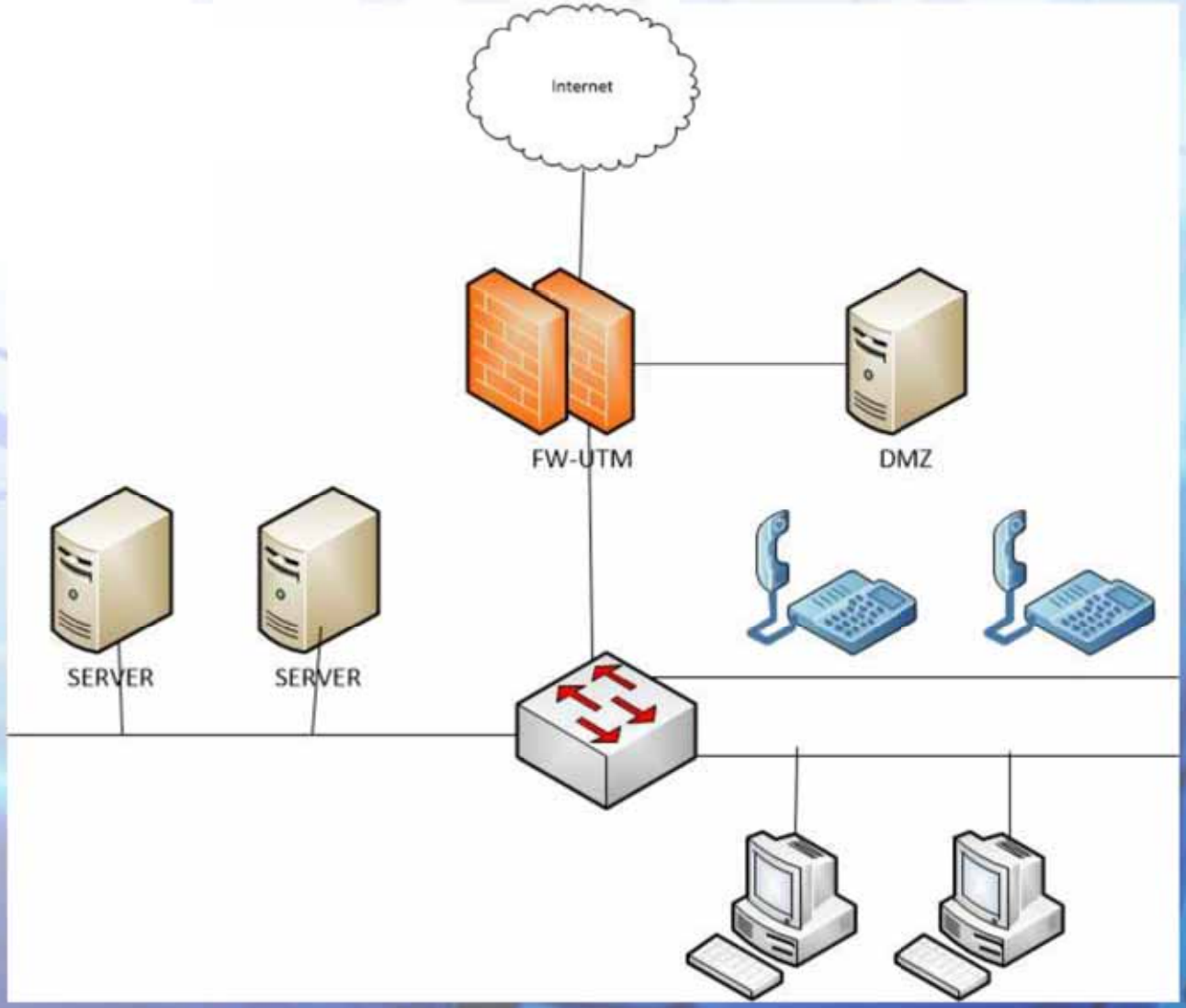
Secur.Net
Always Online, Always Secure!

SOHO



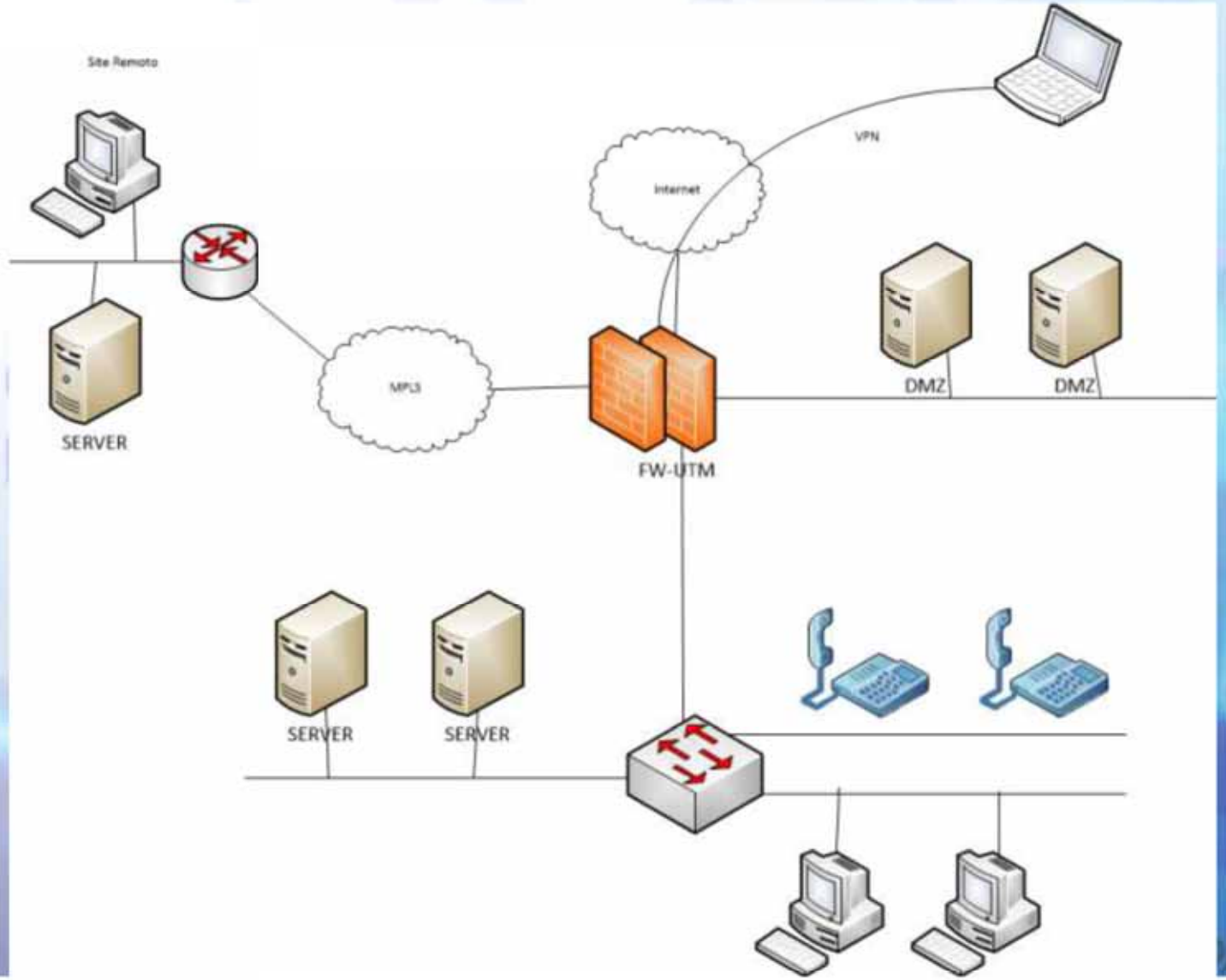
Secur.Net
Always Online, Always Secure!

PME



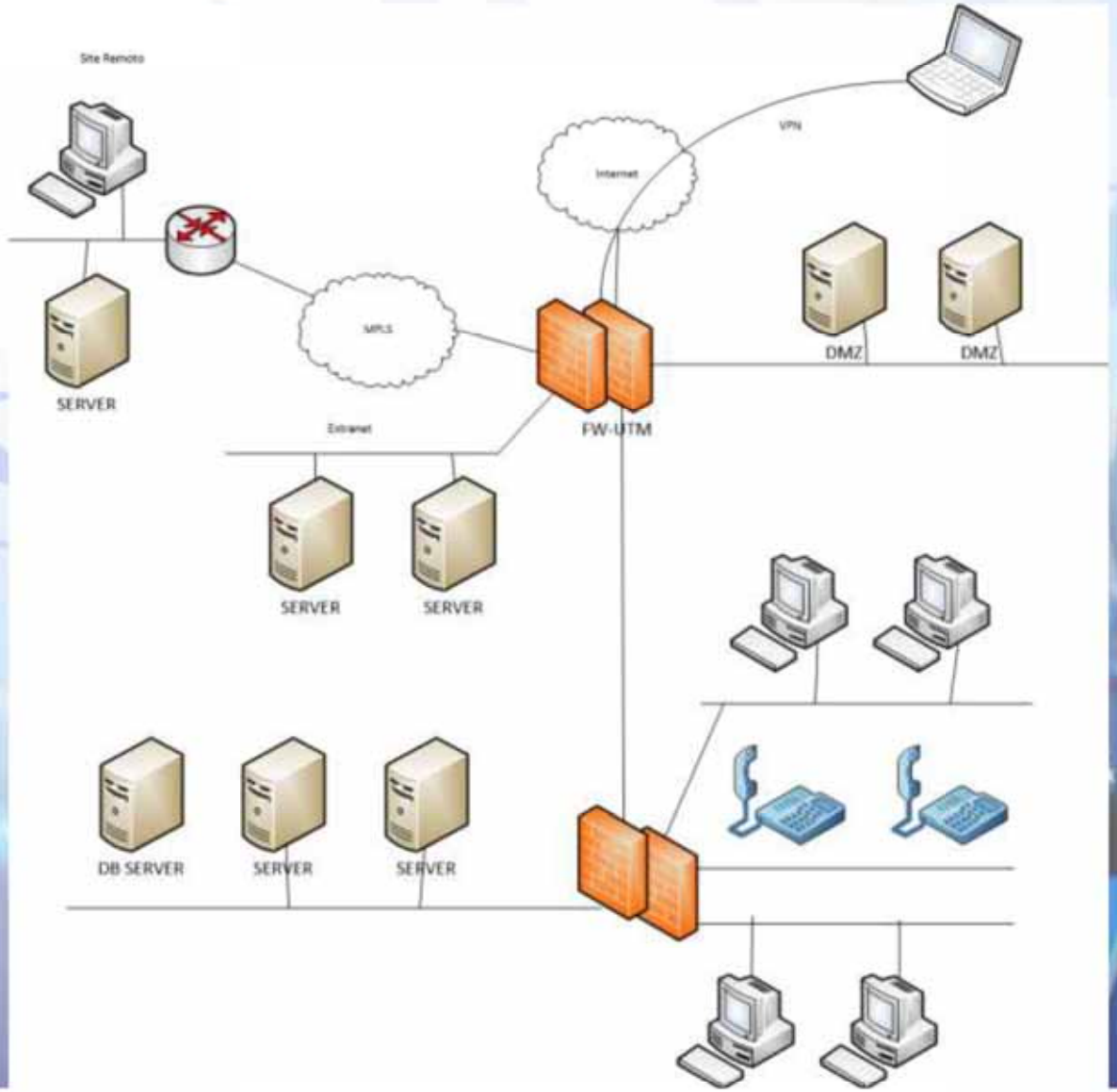
Secur.Net
Always Online, Always Secure!

Corporate



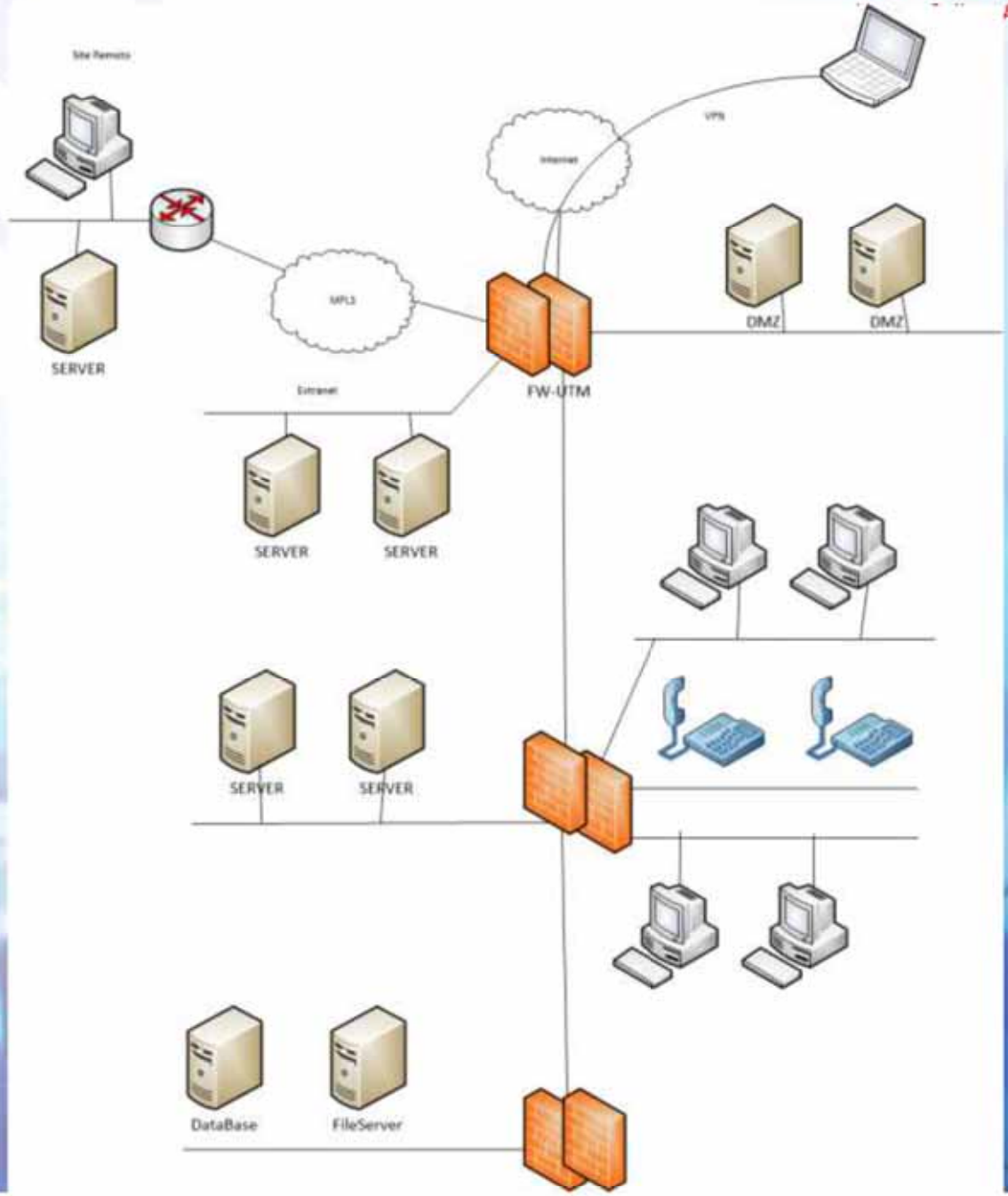
Secur.Net
Always Online, Always Secure!

Corporate w/ Partners Services

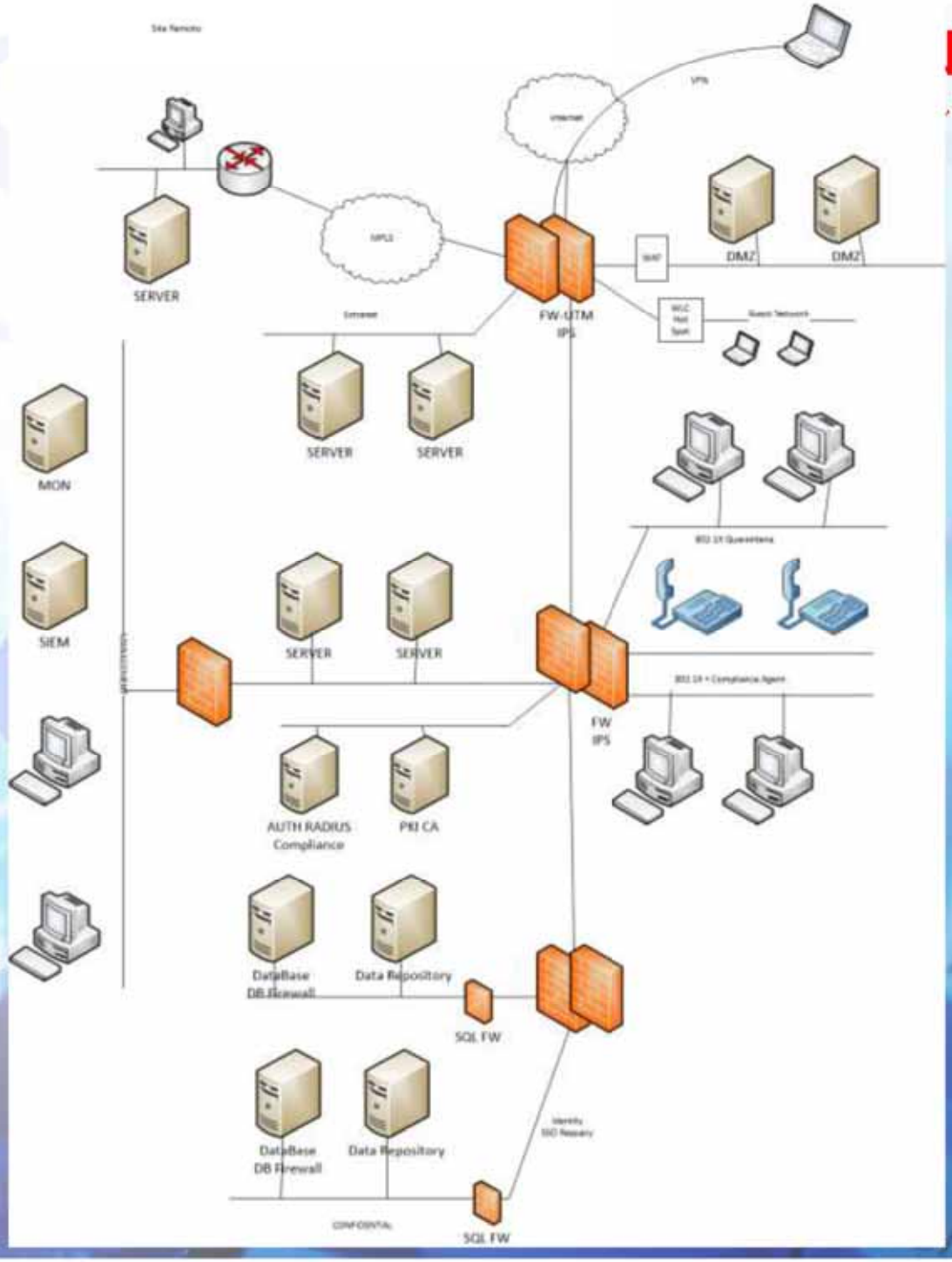


Secur.Net
Always Secure!

Enterprise



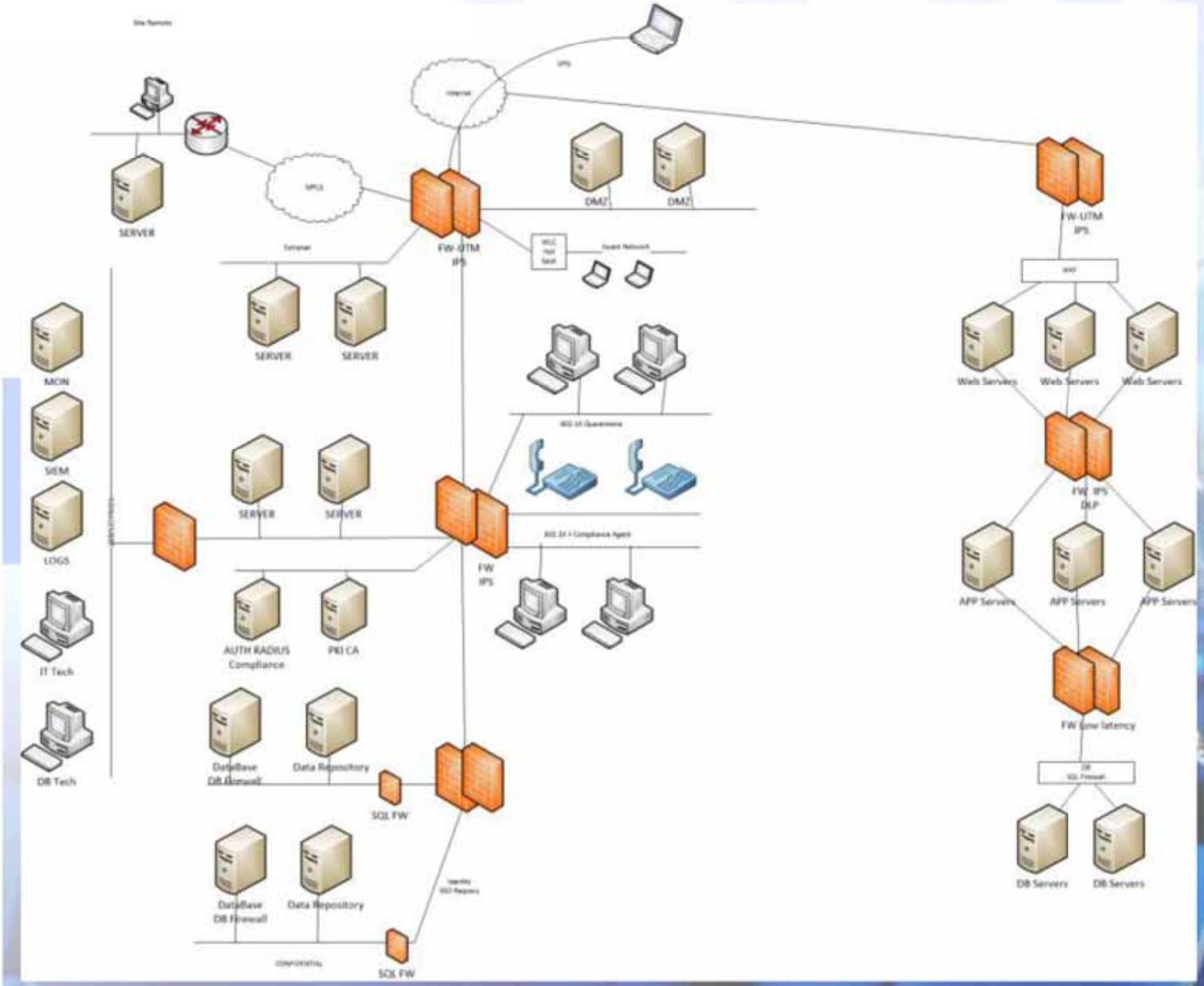
Enterprise w/ Security Dep.



Secur.Net

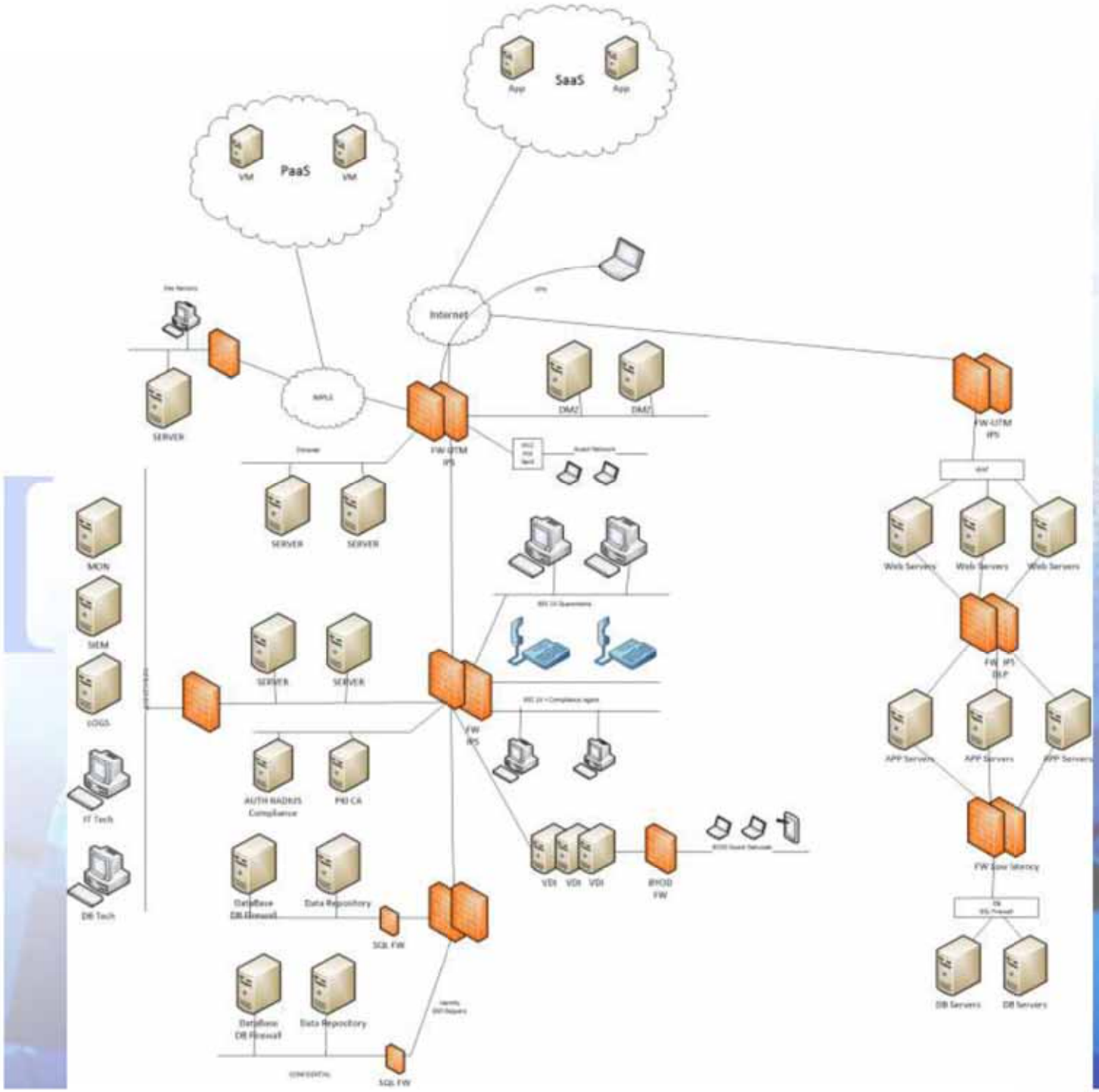
Always Online, Always Secure!

ENTERPRISE w/ Digital Business



Secur.Net

Always Online, Always Secure!



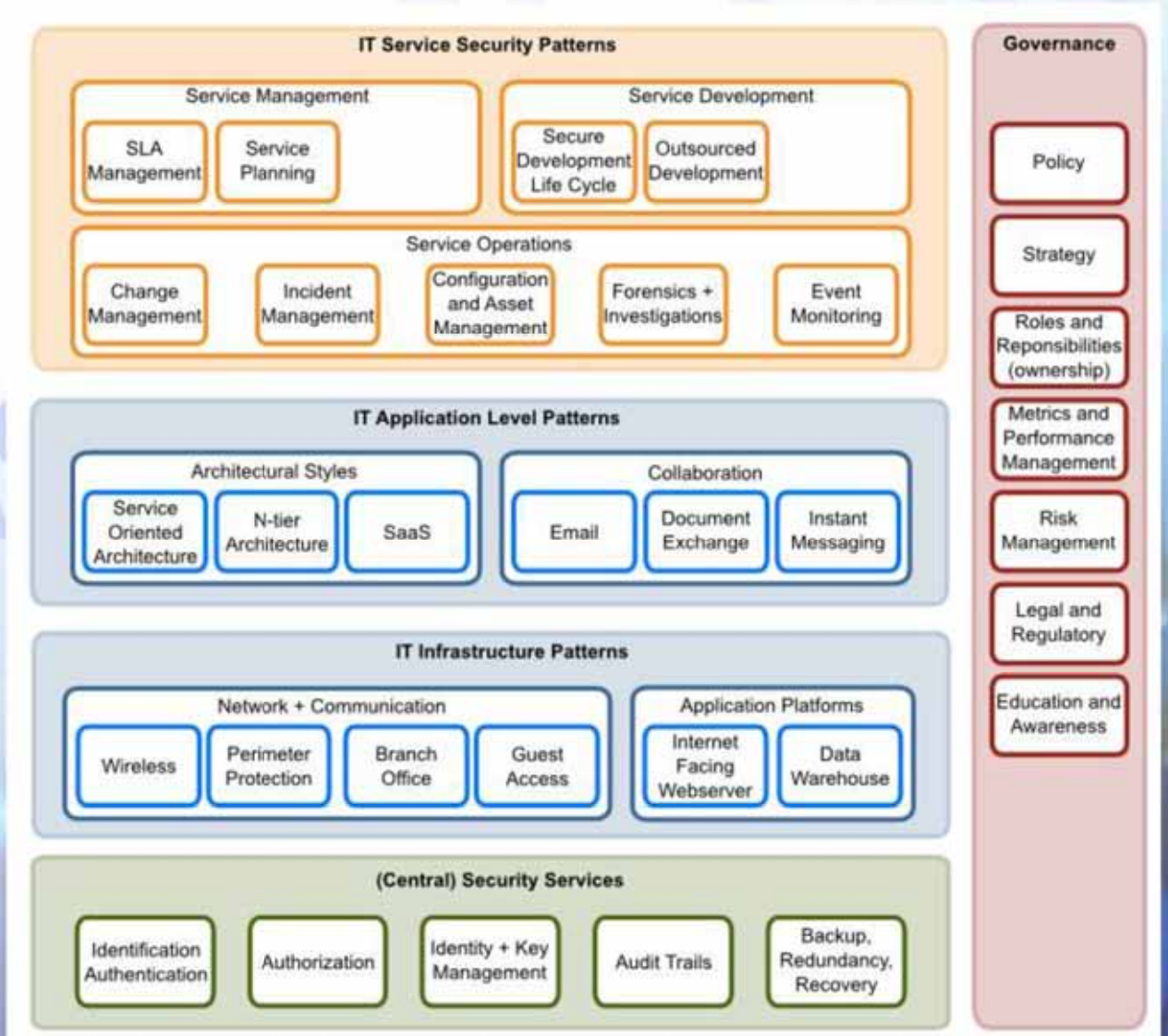
Novos Desafios

- BYOD
- SaaS
- PaaS

Secur.Net
Always Online, Always Secure!

Security Land Scape

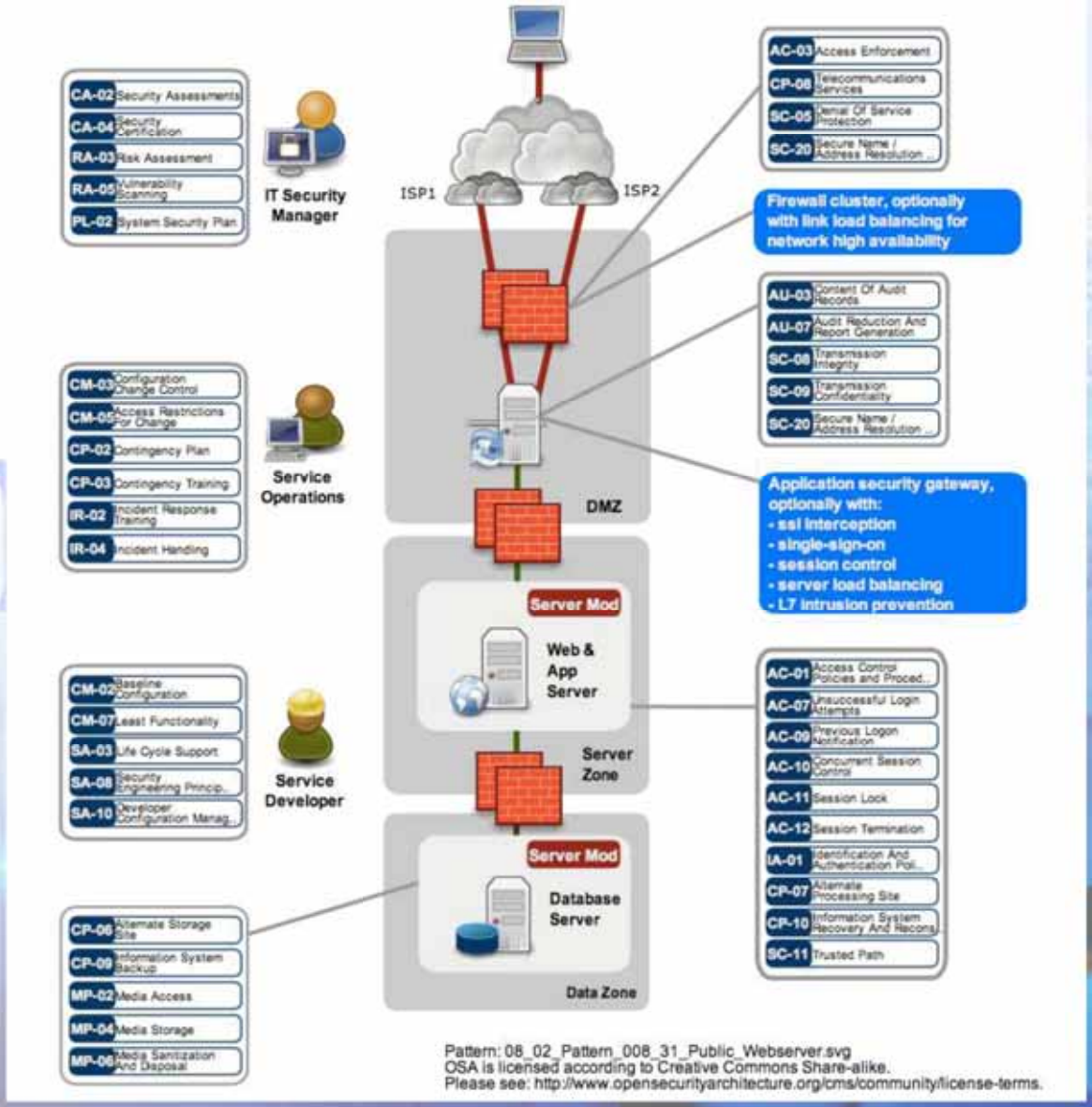
www.opensecurityarchitecture.org



SP-008: Public Web Server Pattern

Secur.Net
Always Online, Always Secure!

Diagram:

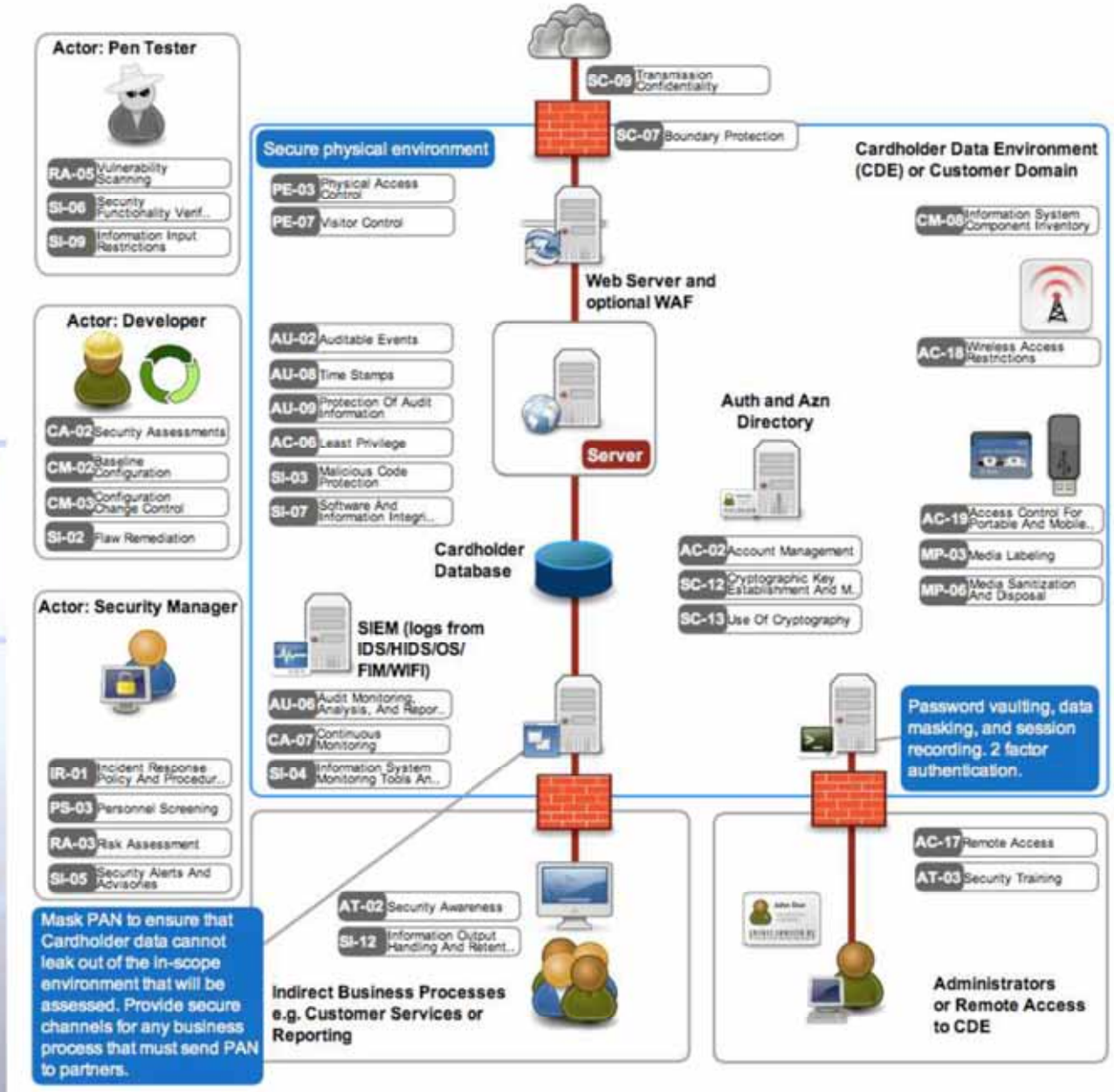


Secur.Net

Always Online, Always Secure!

PCI Enviroment

Diagram:



Exemplo: Doc. Control

SC-09 Transmission Confidentiality

Control: The information system protects the confidentiality of transmitted information.

Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission confidentiality using IPsec. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. Related security control: AC-17.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

Baseline: LOW Not Selected MOD SC-9 HIGH SC-9 (1)

Family: System And Communications Protection

Class: Technical

ISO 17799 mapping: 10.6.1, 10.8.1, 10.9.1

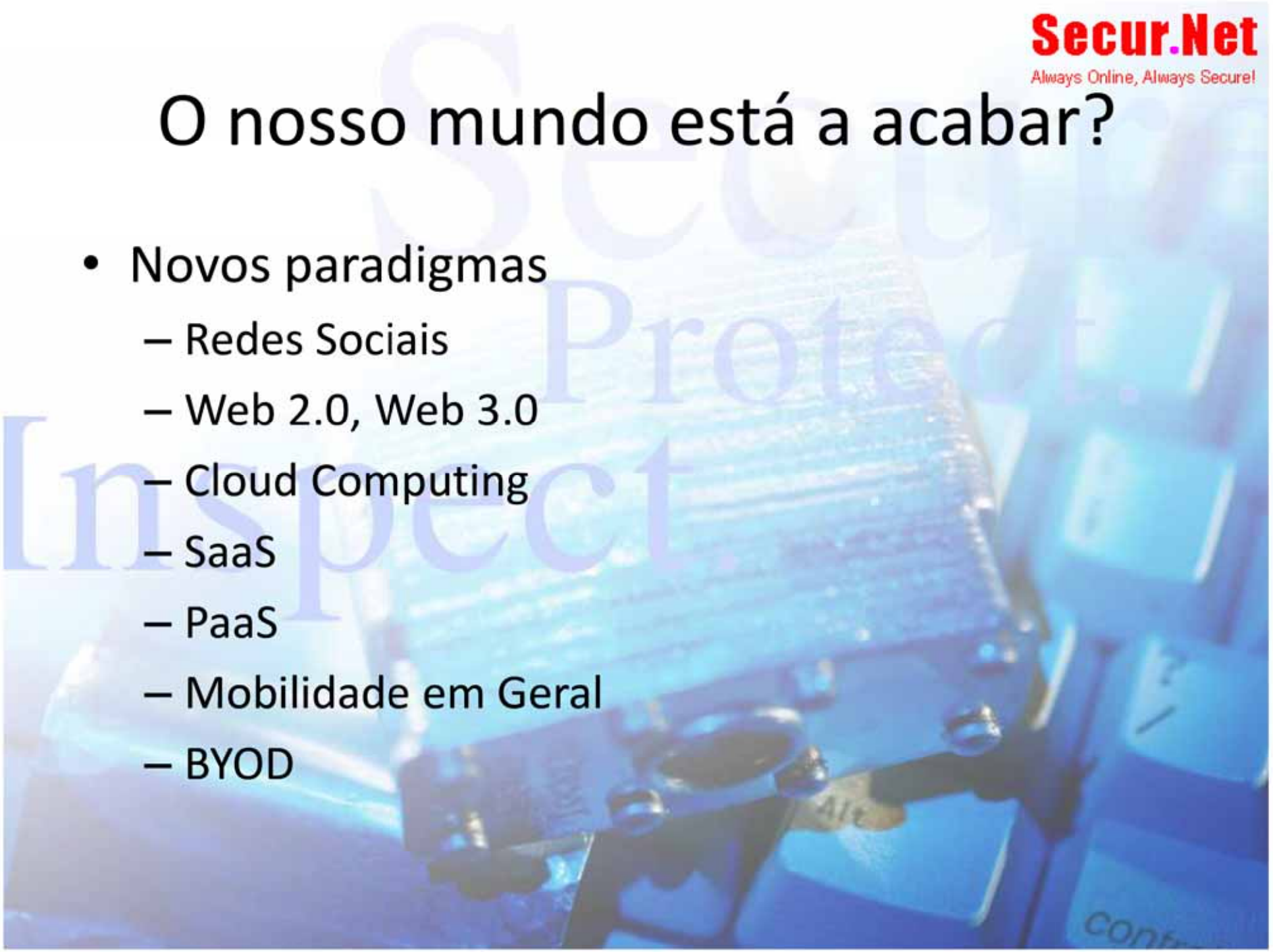
COBIT 4.1 mapping: DS5.11, AC6

PCI-DSS v2 mapping: 4.1, 4.1.1

Secur.Net
Always Online, Always Secure!

O nosso mundo está a acabar?

- Novos paradigmas
  - Redes Sociais
  - Web 2.0, Web 3.0
  - Cloud Computing
  - SaaS
  - PaaS
  - Mobilidade em Geral
  - BYOD



Secur.Net
Always Online, Always Secure!

Não,
Apenas está sempre a Mudar!

Obrigado.

Miguel.Santiago@Securnet.Pt