ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

Resumo

Boas práticas

ISEL – Instituto Superior de Engenharia de Lisboa
Rua Conselheiro Emídio Navarro, 1 | 1959-007 Lisboa

Definir um desenho de rede seguro

- Dificilmente será contruído a partir da raiz
- Normalmente é avaliado o que existe
  - Com uma visão global
- É necessário
  - Definir ativos
  - Definir riscos
  - Calcular orçamento
  - Alocar recursos

Mitigar fatores de risco

- Objetivos:
  - Melhorar a segurança
  - De acordo com o especificado em normas

- Os objetivos devem ser definidos antes do desenho da solução

- Vai ter impacto na arquitetura, custo e complexidade

Plano

- Identificar os ativos
  - Ser o mais completo possível
  - Consultar a administração para determinar expetativas
  - Incluir desktops
    - Mesmo sem dados, existe um custo da sua recuperação
- Visualmente apelativo, espalhar $$$ num mapa de rede
- Identificar pontos de ataque
  - Identificar a possibilidade dos ataques
  - Alocar recursos de acordo com estes

Quais são os riscos?

- Qualquer sistema como acesso direto ou indireto à Internet é suspeito
  - Os desktops são um canal para recursos valiosos
    - Os utilizadores com acesso à Internet ligam-se a servidores internos
  - Ferramentas de segurança processam dados não fidedignos
    - Se a *firewall* fosse comprometida conseguimos detetar?
- O risco não são os portos abertos para a Internet, mas sim os sistemas que são comprometido através destas

Definir as zonas de segurança

- Uma zona é um segmento único segregado
- Segregar os ativos baseados no seu valor
- Segregar os ativos baseados no seu grau de confiança
- Valor mais elevado leva normalmente a maiores graus de confiança
- Atribuir um grau de confiança a cada zona

Estratégia

Nível da rede

- Router de fronteira
  - Utilizar *supernetting* para sumarizar todas as redes
  - Deve ser um dispositivo isolado
- Firewall dinâmica
  - Valida o tráfego
  - Valida os protocolos e NAT apenas
  - Evitar soluções UTM e ambientes virtualizados partilhados
  - Visibilidade do que entra e sai da rede
    - É o melhor local para detetar *hosts* comprometidos

Estratégia

Nível do cabo

- Filtragem ao nível da aplicação
  - Utilizando proxies
    - Reverse proxy, SMTP gateway, ...
  - NIPS quando a velocidade ou complexidade é uma preocupação
- Monitorização da camada de rede
  - NIDS
  - Pode fornecer alertas

Estratégia

Switching

- Tomar atenção às zonas de fronteira
  - Switches físicos diferentes quando
    - Existir uma diferença muito grande quando as zonas têm graus de confiabilidade muito diferentes
  - VLANS em zonas com graus de confiabilidade próximos

- Não criar caminhos alternativos à volta de uma *firewall* ou filtro

Estratégia

Virtualização

- Todos as máquinas virtuais devem ser da mesma zona de segurança
- Evitar *hosts* que atravessem multiplas zonas de segurança
  - A *firewall* é um bom exemplo
  - Mas colocar uma zona virtual atrás de uma zona melhora a segurança
- Permitir que o *host* monitorize as máquinas virtuais

Estratégia

VPNs e Cifra

- Evitar VPNs a terminar em sistemas
  - Terminar VPNs na fronteira
- Cifra para dados em circulação
  - Sempre que atravessa zonas de baixo grau de confiança
- Cifra para dados armazenados
  - Sempre que o recurso possa ser perdido ou roubado

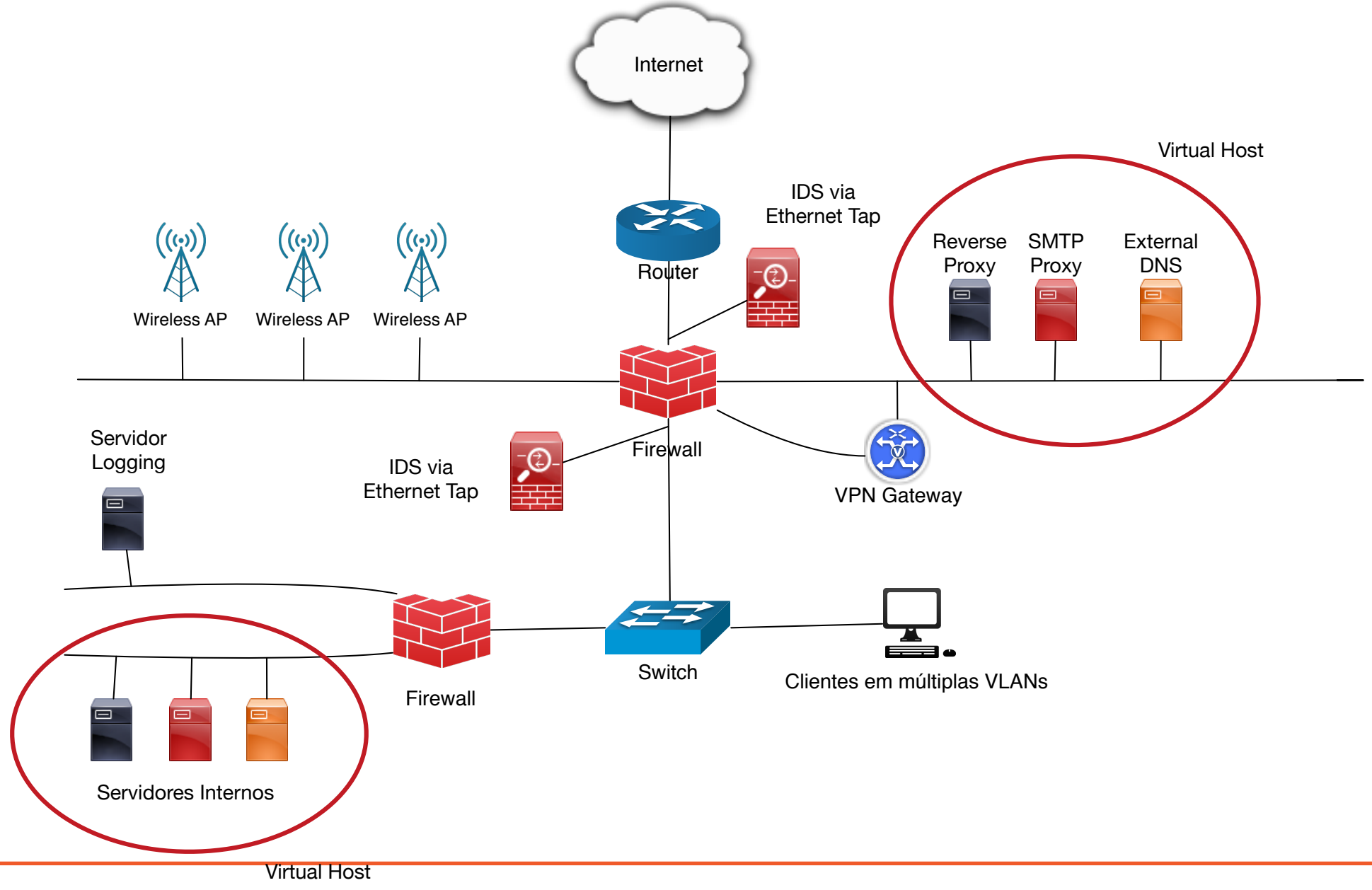
Estratégia

Logging

- Quando for colocado em produção é preciso pensar na manutenção a longo prazo
- Isolar o equipamento
- Cifrar registos que atravessem zonas de baixo grau de segurança
- Focar na qualidade e não na quantidade
  - Registar dados úteis de muitos sistemas é mais útil que tudo de poucos sistemas
  - Num mundo ideal queremos tudo

Estratégia
Auditoria e Análise Forense

- Especificar a auditoria
  - Comprar os *hosts* com estados anteriores conhecidos como "bons"
  - Pode simplificar e acelerar o processo de auditoria
  - Ultima linha de defesa
- Definir objetivos forenses
  - Determinar ponto de entrada
  - Determinar extensão do ataque


Internet
Virtual Host
IDS via
Ethernet Tap
Router
Reverse
Proxy
SMTP
Proxy
External
DNS
Wireless AP
Wireless AP
Wireless AP
Servidor
Logging
IDS via
Ethernet Tap
Firewall
VPN Gateway
Switch
Clientes em múltiplas VLANs
Firewall
Servidores Internos
Virtual Host