Gestão de equipamentos de rede: Olhar de segurança

Autores:
Gustavo Ramos
Artur Renato

GTS - Grupo de Trabalho em Segurança de Redes - 22ª Reunião
São Paulo, SP - 6 de dezembro de 2013

PINPOINT

IPivot Telecom

Motivação

- A equipe de **redes** entende de **segurança**?
- A equipe de **segurança** entende dos equipamentos de **rede**?
- Três características básicas da Segurança da Informação:
  - Confidencialidade;
  - Integridade;
  - Disponibilidade.
- Aspectos de segurança dos **equipamentos** de rede.
  - Não estamos falando da REDE.

Agenda

- Administração
- Configuração
- Interdomínio
- Processos
- Software e Hardware

Administração (1)

- **Métodos de Autenticação**
  - Gestão de usuários
    - E quando o funcionário sai da empresa?
  - Tacacs? Radius? LDAP? Two-factor?
  - Proxy?
  - Controle de acesso baseado no endereço IP de origem.
  - Definir um procedimento para senha “default”/root/admin/etc.
  - Política de acesso limitada por grupo de usuário (role-based access controls).
  - Política de qualidade de senhas.
  - Notificação automática em caso de violação de algum item da política.

Administração (2)

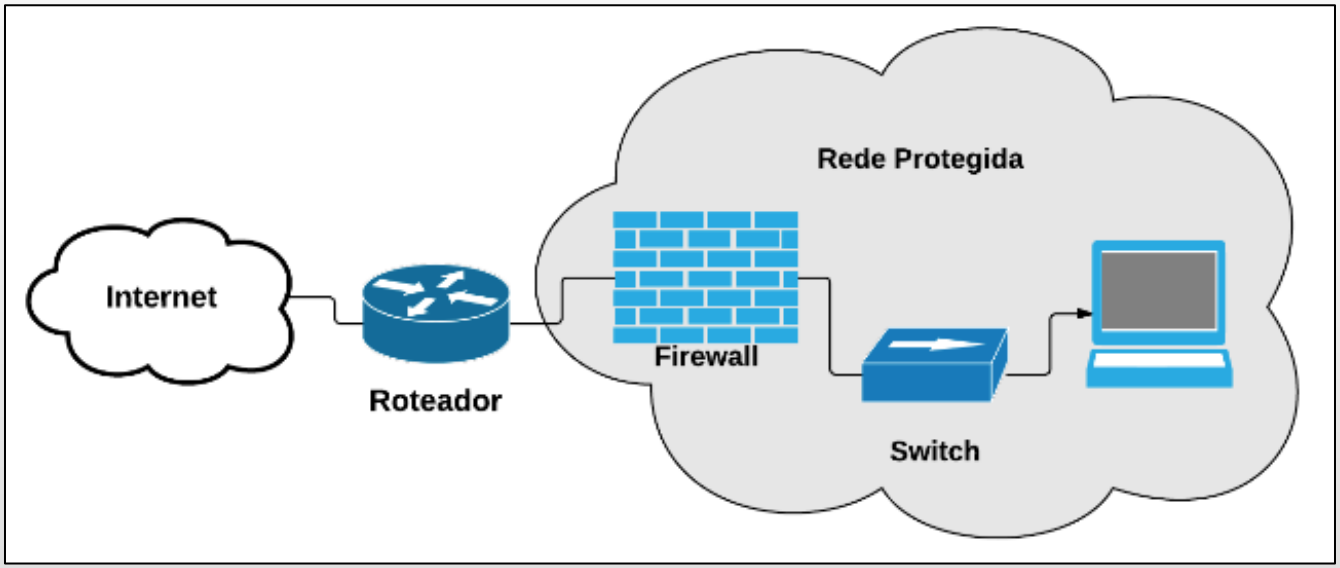
- **Syslog e SNMP Traps**
  - Definir as regras através da exclusão de itens não necessários.
  - Importante para correlação de eventos e análise *post-mortem.*
- **Sistema de Monitoração**
  - Qual é o impacto de um evento?
  - Lembrar-se de monitorar parâmetros pouco comuns: taxa de pacotes/segundo unicast e non-unicast, backplane, etc.
- **Gerência Out-of-Band**
  - Vulgo “tiro no pé”

Configuração

- **Controle dos protocolos utilizados e não utilizados**
  - Desabilitar protocolos não utilizados.
  - Implementar métodos de autenticação e controle.
    - OSPF, HSRP, SNMP, CDP, MNDP, etc.
  - Aplicar filtros e controles para protocolos não-autenticados, por exemplo, Spanning-tree .
- **Backup de Configuração**
  - Definição do(s) horário(s) de backup baseado na política de mudança.
  - Controle de versões.
  - Auditoria automática para detectar alterações não autorizadas.
  - Aplicação de rollback em caso de problema.
- **Auditoria externa na rede**
  - Está realmente atualizada?
  - Analisa os elementos (configurações, protocolols, hardware, etc) que realmente estão em uso?

Interdomínio (1)

- O firewall já controla todo o tráfego destinado a rede interna ou DMZ.
  - **E antes do firewall?**



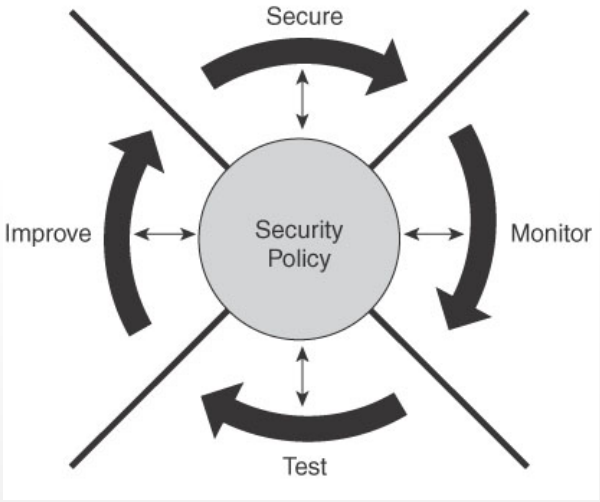
Interdomínio (2)

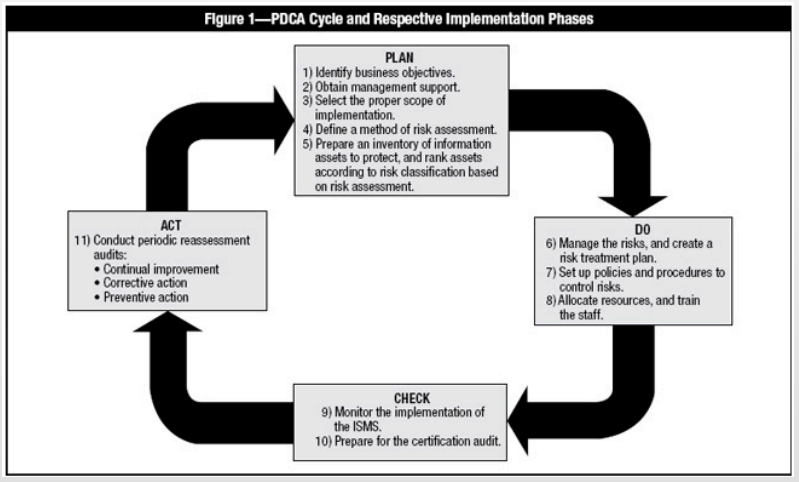
Cuidados ao conectar-se a uma rede de terceiros.

- **Camada 1**
  - Problemas elétricos ou físicos.
- **Camada 2**
  - Metro-ethernet: confiar nos BPDU's de equipamentos de terceiro?
  - Sempre utilizar filtros e controles para o tráfego L2:
    - Filtros de spanning-tree
    - Storm-control
    - Controle de recursos limitados (por exemplo, número máximo de endereços MAC).
- **Camada 3**
  - Escolher um protocolo que permita autenticação e filtros.
    - Utilizar BGP "privado" em caso de interconexão de redes com protocolo de roteamento dinâmico.

Processos

- Definir corretamente uma configuração básica (**baseline**)
- Garantir que os equipamentos estejam configurados de acordo com a política (**checklist**)
- Implementar processos de **Gerência de Mudanças** (GMUD)
  - Normalmente apoiado por uma ferramenta
- Definir um padrão de **documentação da rede**, antes e após a execução de mudanças.





Software e Hardware (1)

- Homologação do Sistema Operacional e *patches*
  - Controle de versões instaladas nos equipamentos em produção
  - Plano de atualização alinhado com os fabricantes de equipamentos
- Gestão de capacidade dos equipamentos
- Planos de Dados e Controle
  - Problemas:
    - Capacidade afetando gerenciamento
    - (D)DoS
  - Possíveis soluções:
    - Definir limites e filtros específicos para o plano de controle (CoPP ou control plane policing)
    - Especificar quais protocolos são prioritários em enlaces críticos (QoS)

Software e Hardware (2)

- Monitoração da Temperatura
- Acesso físico ao Hardware
  - Roubo
  - Danificação
  - Acesso lógico facilitado

PINPOINT

IPivot Telecom

Comentários? Perguntas?

Obrigado!

Contato:

gustavo@pinpoint.com.br

artur@pinpoint.com.br

PINPOINT

IPivot Telecom