



Tópico 13 – Firewall

Ferramentas de defesa - Firewall. Princípios de projeto de firewall. Sistemas confiáveis. Critérios comuns para avaliação de segurança da tecnologia da informação.

Firewalls

O que é um firewall?

Firewalls

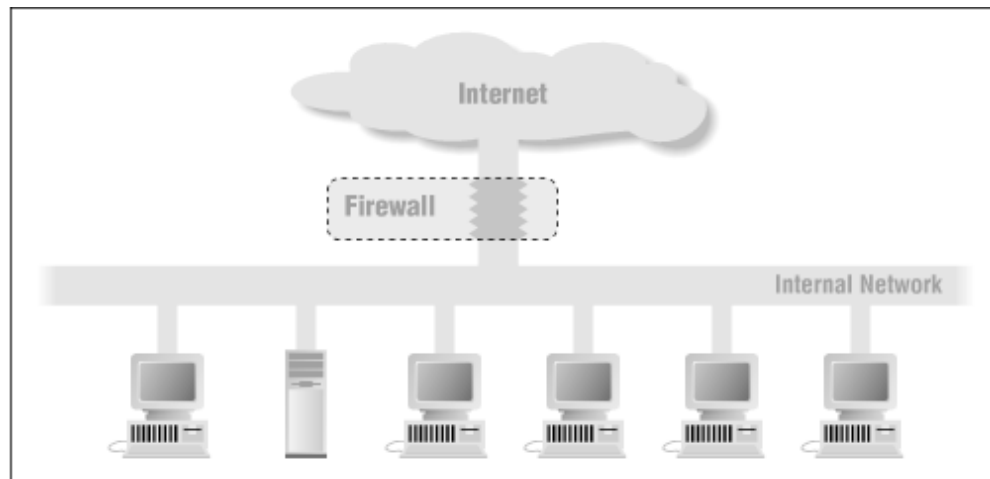
- Uma combinação de hardware e software que forma uma barreira entre uma rede confiável e outra não confiável
- Configuração de rede visando a proteção de uma rede local
- Sistema desenhado para controle de acesso a recursos a partir de uma rede não confiável
- Método de proteção de redes privadas mediante análise do tráfego de entrada e saída

Firewalls

Um firewall é toda estrutura posicionada entre uma rede que se quer proteger e um meio hostil.

A missão do firewall

- O firewall geralmente se coloca entre uma rede a proteger e outra considerada hostil.
- Há casos porém, de firewalls que consideram as duas redes como sendo hostis e protegem uma da outra.



O que um firewall é capaz de fazer?

- Ser um ponto de controle de tráfego
- Aplicar políticas de segurança
- Registrar atividade suspeita
- Limitar a exposição dos ativos e dados

O que um firewall não faz?

- Proteger contra ataques “internos”, salvo em soluções de maior custo
- Controlar tráfego que não passa pelo mesmo
- Proteger contra ameaças “0-day”

Definições

- Bastion Hosts
- Rede de perímetro ou DMZ
- Roteadores de Borda
- Screened Subnets
- Intranet, Extranet
- SOCKS
- Proxy, Filtros de pacotes, Stateful Inspection
- NAT , PAT

Topologia Segura

Uma arquitetura de Rede Segura começa com uma

Topologia Segura

A segregação de Redes de forma adequada é o primeiro passo para uma rede segura e de boa performance, a palavra chave _____

PLANEJAMENTO

Topologia Segura

Basta segregar rede Interna da Internet ?

NÃO

PARADIGMA – REDE INTERNA SEGURA

Atualmente a maioria dos ataques parte da rede Interna, dessa forma a utilização de DMZs internas, e redes segregadas é fundamental para a segurança da rede interna.

Topologia Segura

- Segregação de Redes.
 - ...dividir em diferentes domínios de rede lógicas...
 - ...perímetro de segurança definido.
 - ...domínios devem ser definidos com base em avaliação de riscos...
 - ... baseado na política de controle de acesso e requisitos de acesso

Bastion Hosts

- Host mais exposto da rede
- Mais suscetível a ataques, o bastion host deve ser configurado para sofrer ataques
- Técnicas de OS Hardening muito utilizadas
- Normalmente, os bastion hosts são provedores de serviços ao mundo externo, à frente do resto do firewall

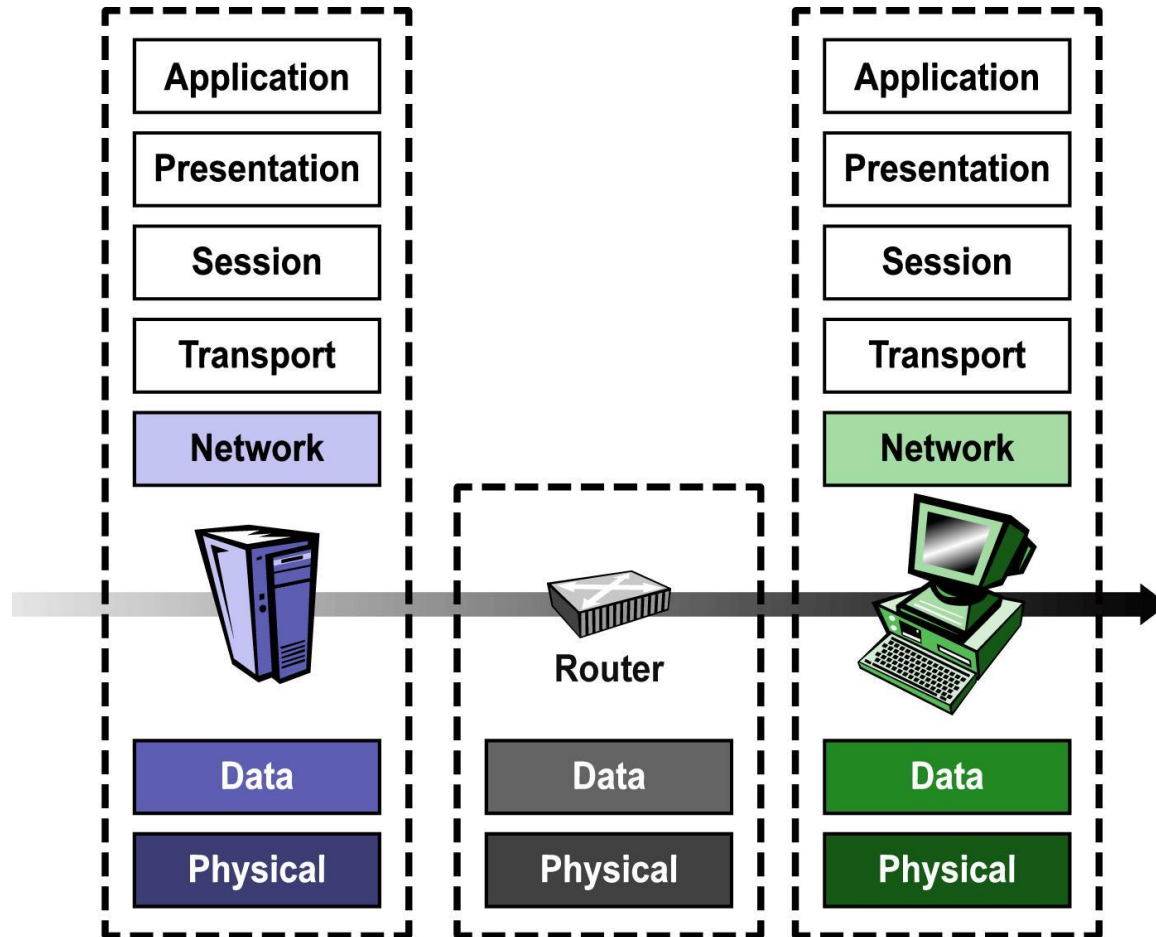
DMZ

- “Demilitarized Zone”, ou zona desmilitarizada, nome que surgiu durante a Guerra da Coreia
- Rede de perímetro. Todo tráfego que passar por esta região será rigorosamente analisado
- DMZ é toda a área dentro do sistema de firewall, ou seja, entre a rede hostil e a rede privada.
- Pode conter serviços
- A rede privada não tem acesso direto à rede hostil, e sim via DMZ, e vice-versa

SOCKS

- O serviço de SOCKS mascara conexões na camada de transporte
- Definido na RFC 1928
- Transparente aos extremos das conexões
- Não faz consulta a DNS
- Mecanismos de log
- Mais inteligente que NAT
- Seguro
- Somente escuta na interface “interna”

Firewalls – Filtros de Pacotes



Firewalls – Filtros de Pacotes

- Vantagens:
 - Custo
 - Transparente para Aplicação
 - Método Rápido

Firewalls – Filtros de Pacotes

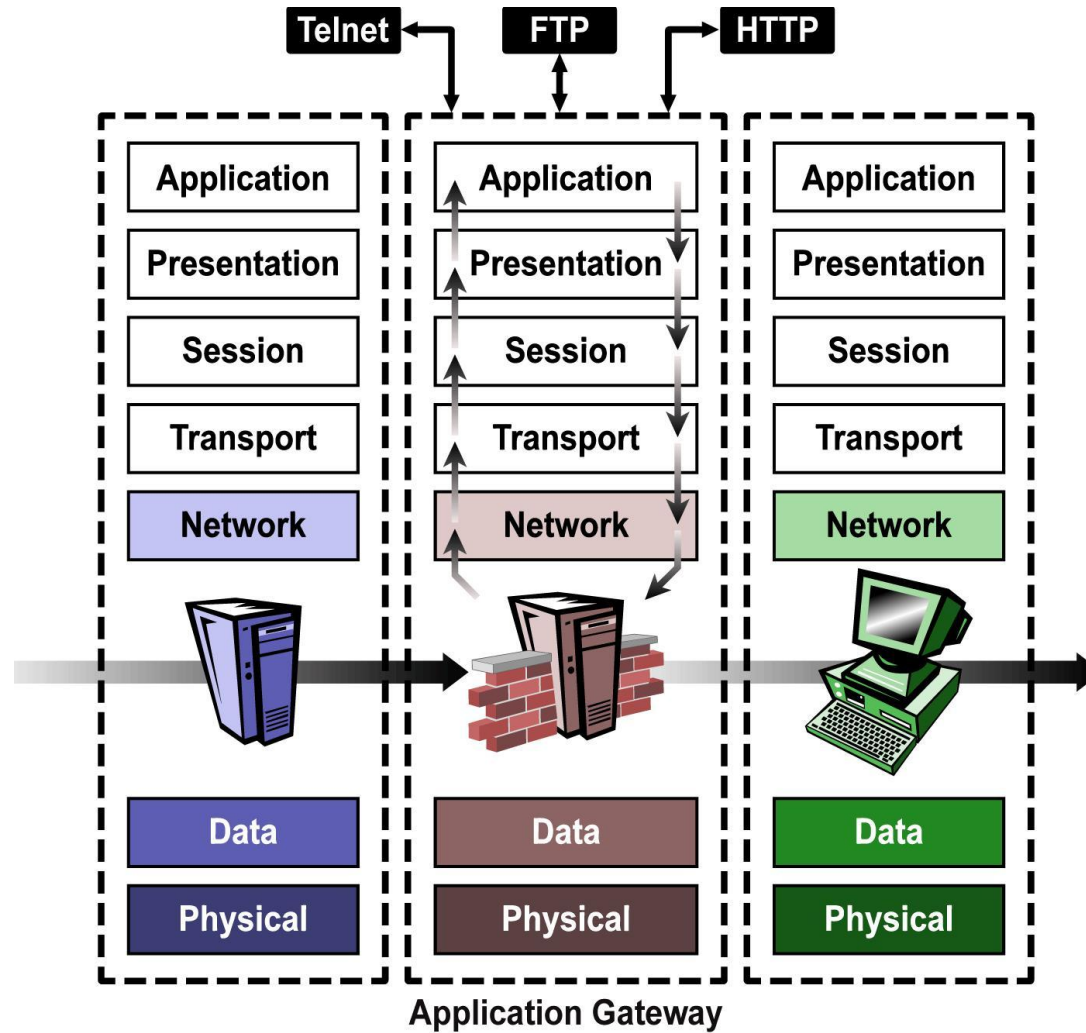
- Desvantagens:
 - Acesso limitado ao cabeçalho do pacote
 - Limitação em manipular informações
 - Difícil de Monitorar e Gerenciar
 - Mínimo mecanismo de Log e Alertas

Firewalls – Filtros de Pacotes

- ACL's CISCO
 - ACL Simples / Extendida

```
Router(config)access-list 11 deny 10.0.0.0 0.255.255.255
Router(config) access-list 101 deny icmp any any
Router(config) access-list 101 permit tcp any host 172.16.100.3 eq 53
Router(config) access-list 101 permit udp any host 172.16.100.3 eq 53
```
- IPChains - LINUX

Firewalls - Proxy



Firewalls - Proxy

- Vantagens:
 - Mais Seguro que ACL's
 - Melhor nível de Log / Gerência
 - Inspeção até camada de aplicação
 - “Quebra” de conexão cliente / servidor

Firewalls - Proxy

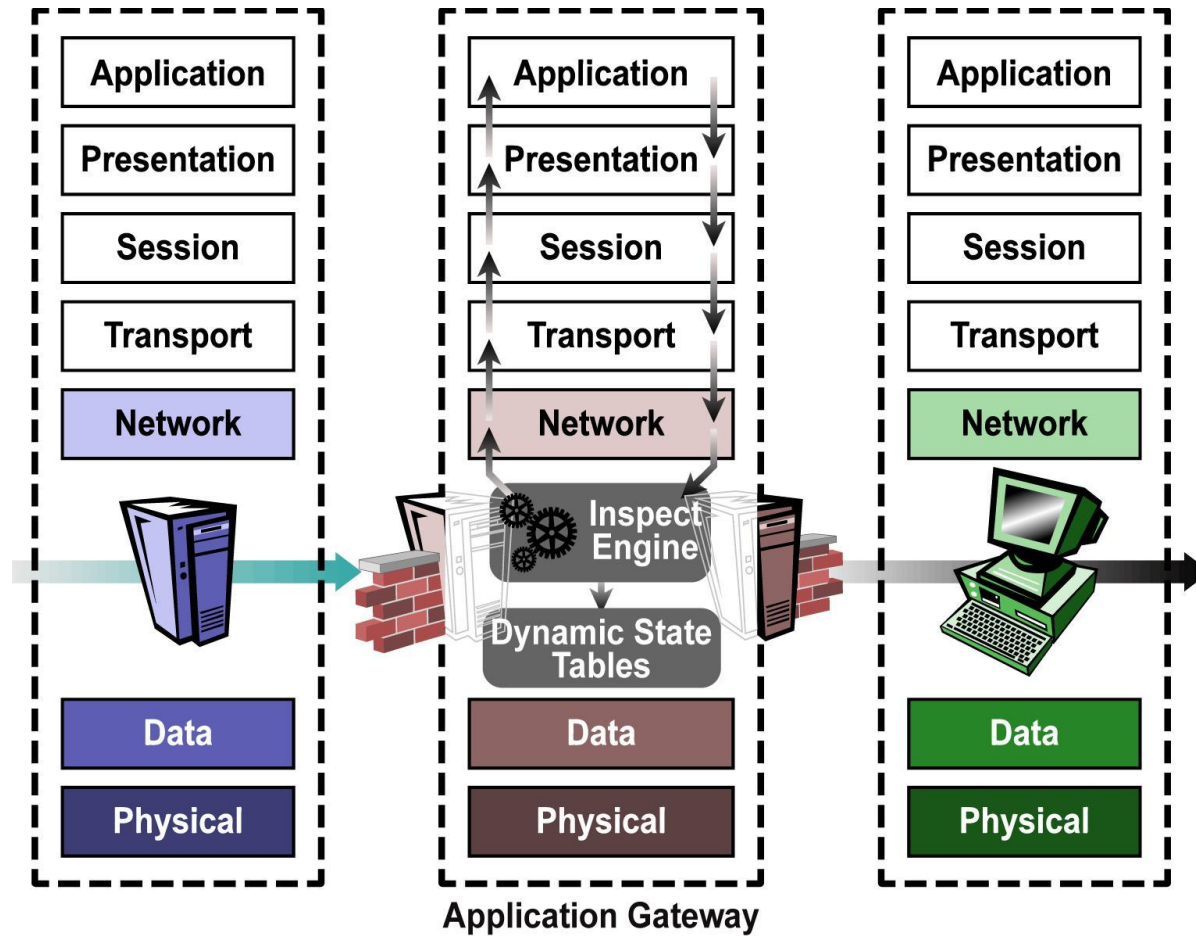
- Desvantagens:
 - Proxy por serviços
 - Escalabilidade
 - Vulnerável a Bugs de SO
 - Número duplicado de conexões
 - Limitação de serviços

Firewalls - Proxy

- Squid
- ISA Server Microsoft
- Outros

.

Firewalls – Stateful Inspection



Firewalls – Stateful Inspection

- Inspeção completa do Pacote
- Controle sobre protocolos não orientados a conexão - UDP, ICMP
- Mais agilidade na inspeção
- Mais confiável (Tabela de Estados)
- Firewall de 3 Geração
- Atualmente estamos na 5 Geração com conceito de Application Firewalls

Firewalls – Stateful Inspection

- Check Point
- CISCO ASA
- IPTables - LINUX

.

Firewalls - Políticas

- Conjunto de Regras = Política
- Imposta por Firewalls e outros dispositivos de perímetro de rede

Firewalls – Políticas

- Restritivas: Tudo o que não é explicitamente liberado está negado
- Permissivas: Tudo o que não é explicitamente negado está liberado.

Firewalls – Players de mercado

CheckPoint

- Seu principal produto, o Firewall-1, foi um dos primeiros a chegar ao mercado
- Líder em grandes corporações
- Interface gráfica para configuração
- Sistemas operacionais
 - Windows
 - Solaris
 - Linux
 - IPSO (Appliances)
 - Secure Plataform (Appliances e Open Servers)

Firewalls – Check Point

- Suporte a tecnologias (OPSEC)
- Stateful Inspection
- Integração com VPN
- Ambiente Cluster
- Protocolos pré-definidos
- NAT
- Autenticação
- Roteamento Dinâmico (Multicast)
- VoIP
- Controle de Aplicações
- 5 Geração

Firewalls – Check Point

Demo Mode - Check Point SmartDashboard R75 - Standard

File Edit View Manage Rules Policy SmartWorkflow Search Window Help

Firewall NAT IPS Application Control Anti-Spam & Mail Mobile Access Data Loss Prevention Anti-Virus & URL Filtering IPSec VPN QoS Desktop

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Stealth	Corporate-internal	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any	Stealth rule - prevent the VPN_firewall host from being scanned or attacked
2	Site to site VPN	Any	Any	All_GwToGw	CIFS ftp-port http https smtp	accept	Log	Policy Targets	Any	Allow site to site VPN traffic
3	Remote access	Mobile-vpn-users	Any	RemoteAccess	CIFS http https imap	accept	Log	Policy Targets	Any	Allow remote access VPN users access to file, web, and print services
4	Clientless VPN	Clientless-vpn-users	Corporate-WA-p	Any Traffic	https	User Auth	Log	Policy Targets	Any	Allow clientless (SSL based) VPN users using certificates from the Security Gateway Internal Certificate Authority
5	Web server	L2TP-vpn-users@Customers@Any	Remote-1-web-s	Any Traffic	http	accept	Log	Policy Targets	Any	Allow partners using Microsoft Win VPN clients or customers to access Remote 1's web server
6	Outbound HTTP	Remote-2-internal	Any	Any Traffic	http	Client Auth	Log	Remote-2-gw	Any	Audit all outbound user HTTP connections from remote-2-internal using UserAuth
7	Critical subnet	Corporate-internal	Corporate-financial Corporate-hr-net Corporate-rnd-net	Any Traffic	Any	accept	Log	Corporate-gw	Any	Log traffic to critical subnets - only enforce this rule on the Corporate-gw

Firewalls - CISCO

ASA Firewall

- Appliance
- Administrado a partir de clientes Windows
- Suporte a tecnologias
- NAT / PAT
- Filtragem em camada de aplicação
- RADIUS/TACACS+
- VoIP

Firewalls- FreeBSD

IPFW

- Ferramenta de filtragem de pacotes
- Incluída no kernel do SO
- Stateful Inspection
- Integração com IDS
- Configuração via texto
- Suporte a autenticação oferecido pelo sistema operacional

Firewalls - Linux

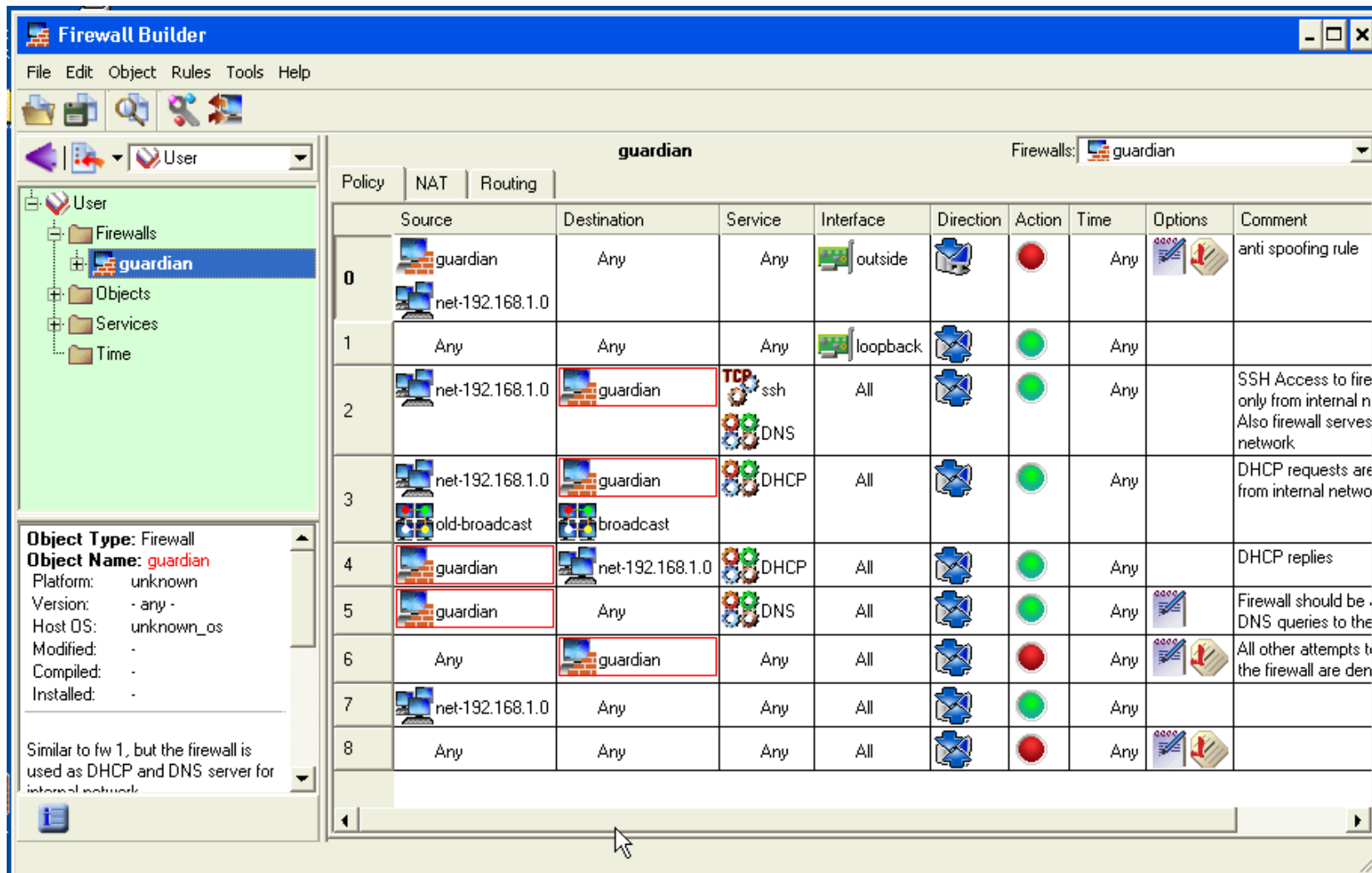
Iptables

- Sucessor do ipfwadm e ipchains
- Ferramenta de filtragem de pacotes
- Incluída no kernel do SO
- Stateful Inspection
- Integração com IDS
- Configuração via texto
- Suporte a autenticação oferecido pelo sistema operacional

Firewalls - fwbuilder

- Ferramenta gráfica para criação de filtros de pacotes
- Open Source
- Suporta diversos tipos de firewalls
- Configuração orientada a objeto, semelhante à da Check Point
- Plugins disponíveis para diversos sistemas

Firewalls - fwbuilder



Firewall Builder

File Edit Object Rules Tools Help

Firewalls: guardian

Policy NAT Routing

	Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
0	guardian net-192.168.1.0	Any	Any	outside		Red circle	Any		anti spoofing rule
1	Any	Any	Any	loopback		Green circle	Any		
2	net-192.168.1.0	guardian	TCP ssh DNS	All		Green circle	Any		SSH Access to fire only from internal n Also firewall serves network
3	net-192.168.1.0 old-broadcast	guardian broadcast	DHCP	All		Green circle	Any		DHCP requests are from internal netwo
4	guardian	net-192.168.1.0	DHCP	All		Green circle	Any		DHCP replies
5	guardian	Any	DNS	All		Green circle	Any		Firewall should be . DNS queries to the
6	Any	guardian	Any	All		Red circle	Any		All other attempts to the firewall are den
7	net-192.168.1.0	Any	Any	All		Green circle	Any		
8	Any	Any	Any	All		Red circle	Any		

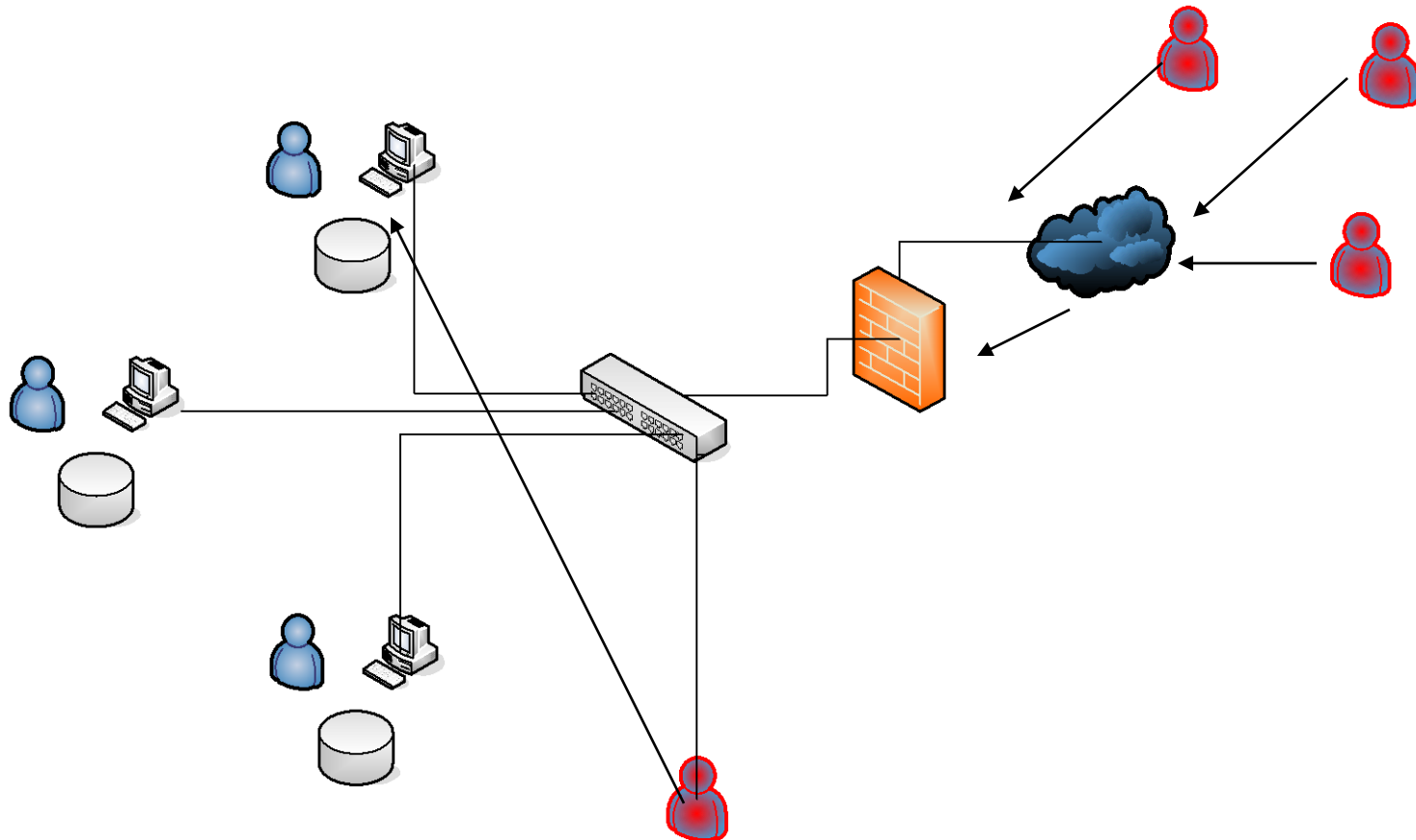
Object Type: Firewall
Object Name: guardian
 Platform: unknown
 Version: - any -
 Host OS: unknown_os
 Modified: -
 Compiled: -
 Installed: -

Similar to fw 1, but the firewall is used as DHCP and DNS server for internal network

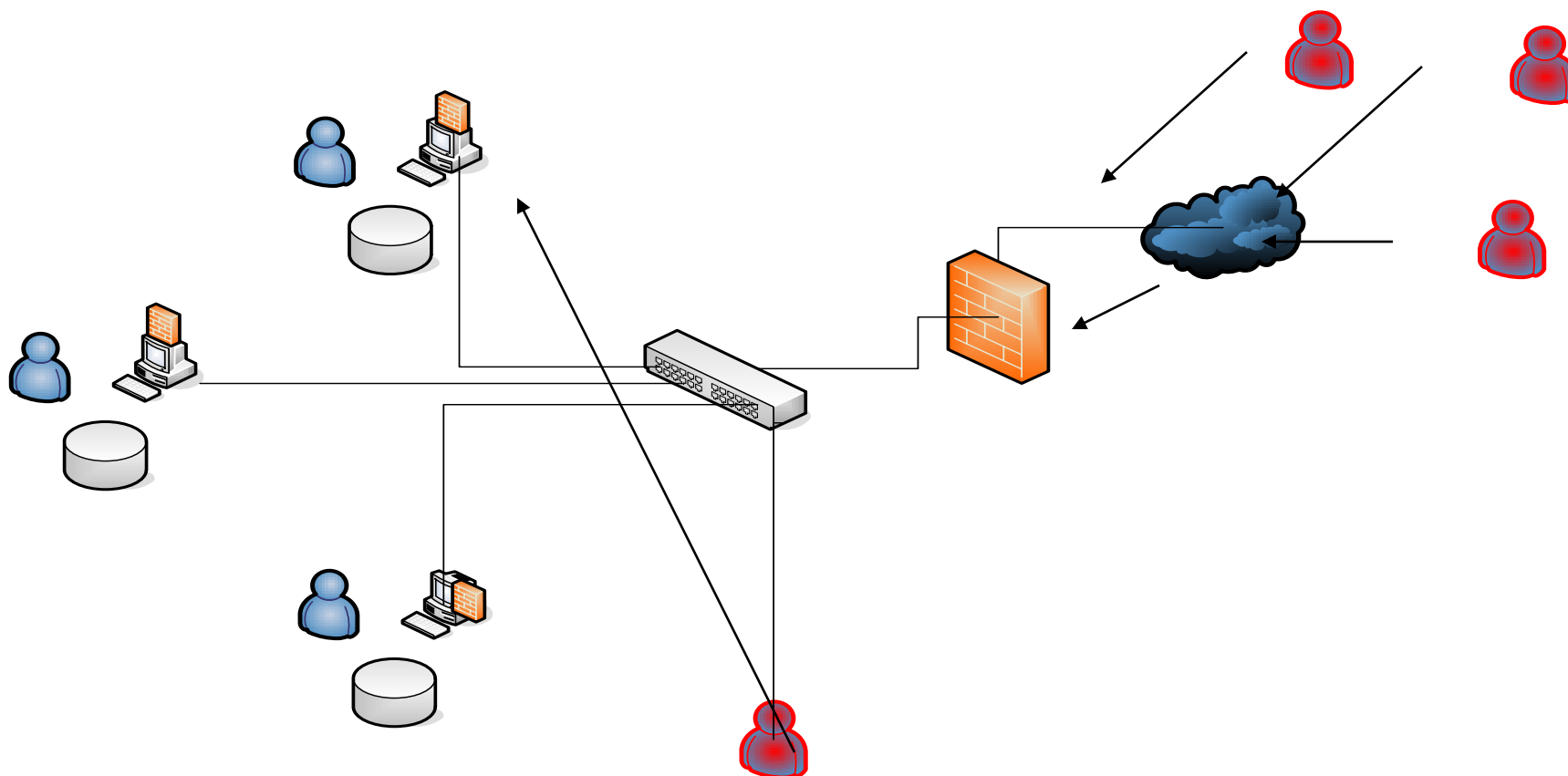
Outros players / produtos

- Microsoft – ISA Server
- Juniper Networks
- Fortinet
- Symantec
- Sonicwall
- Aker

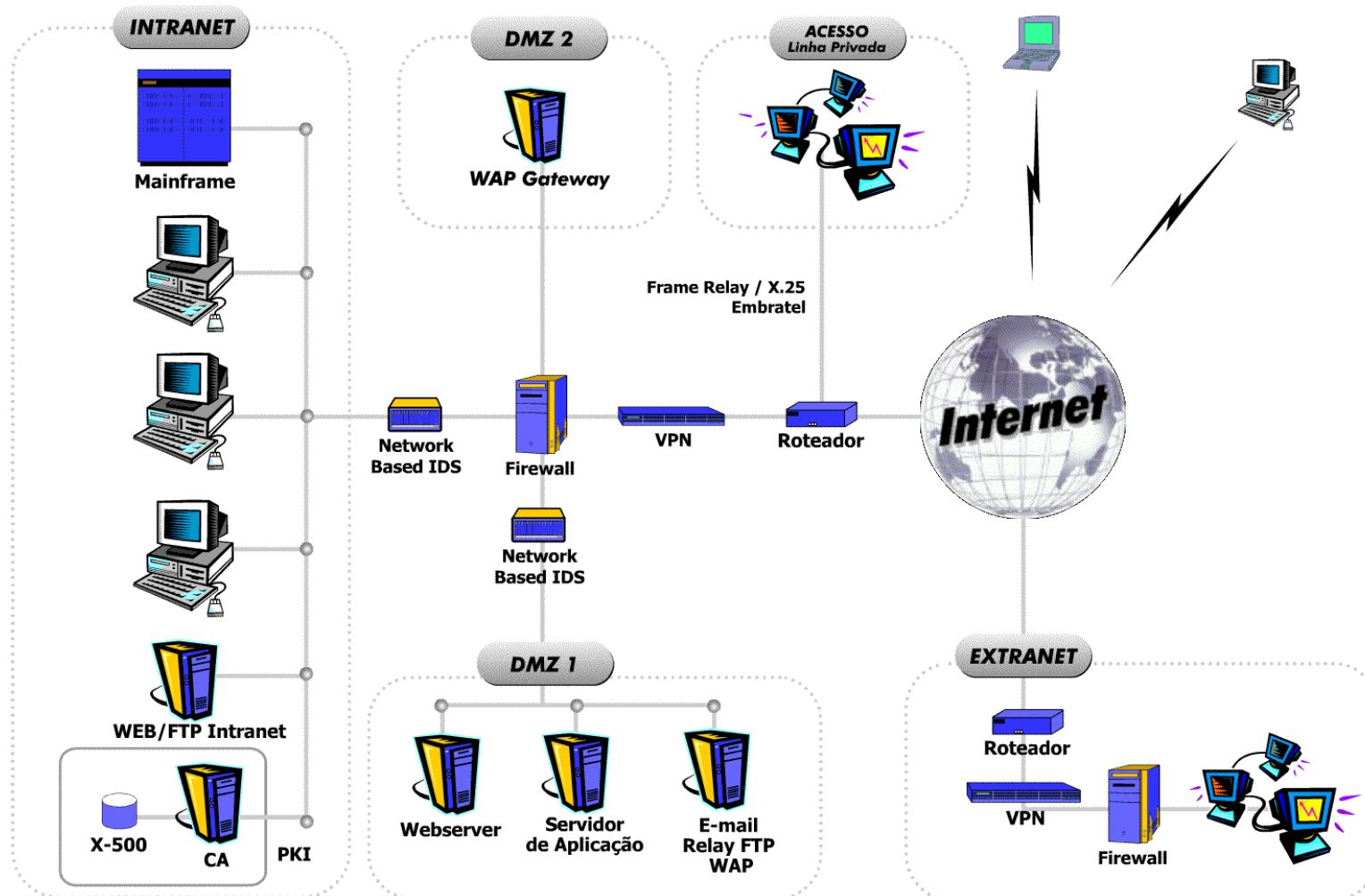
Host Firewall x Network Firewall



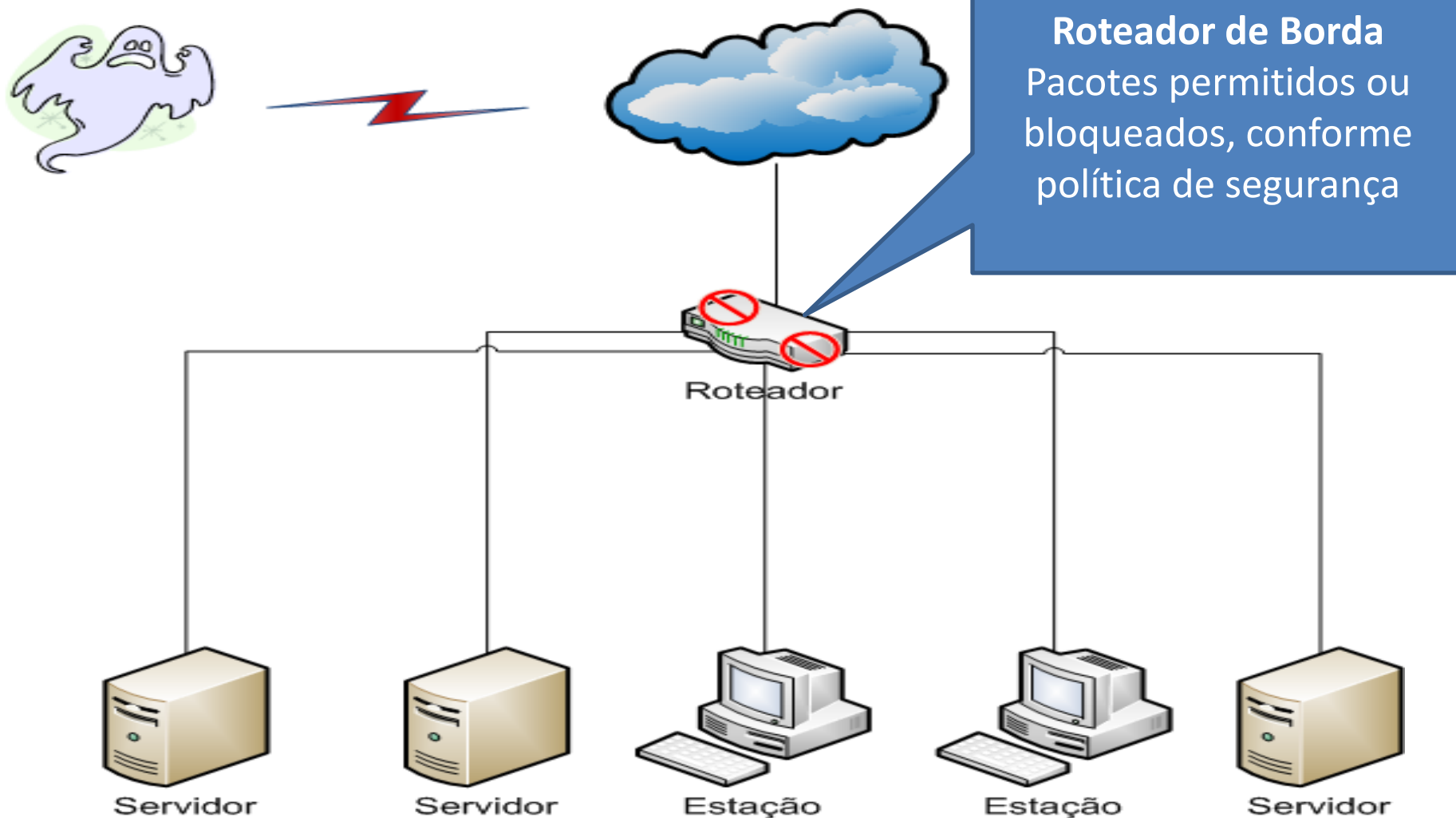
Host Firewall x Network Firewall



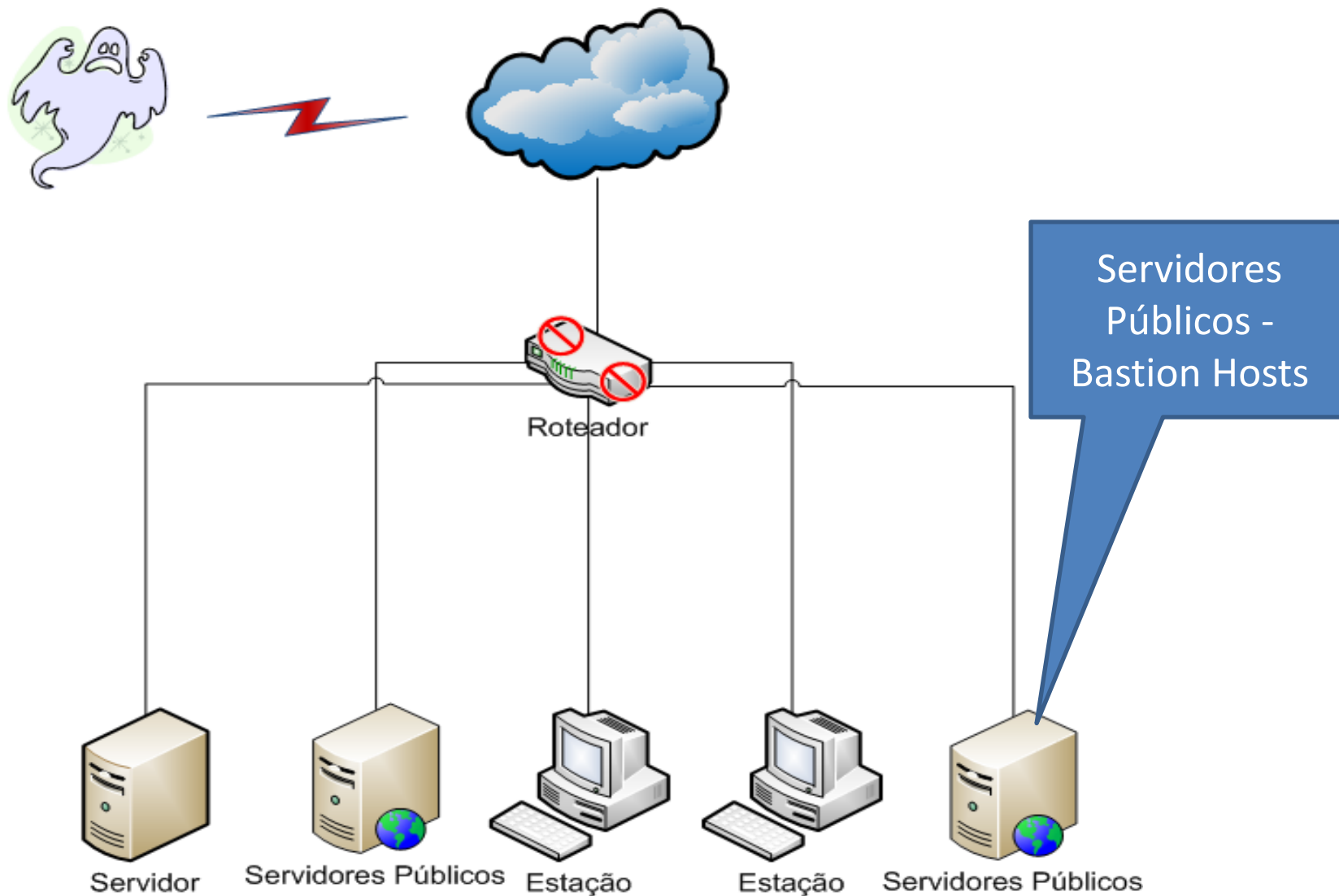
Firewalls -Perímetros



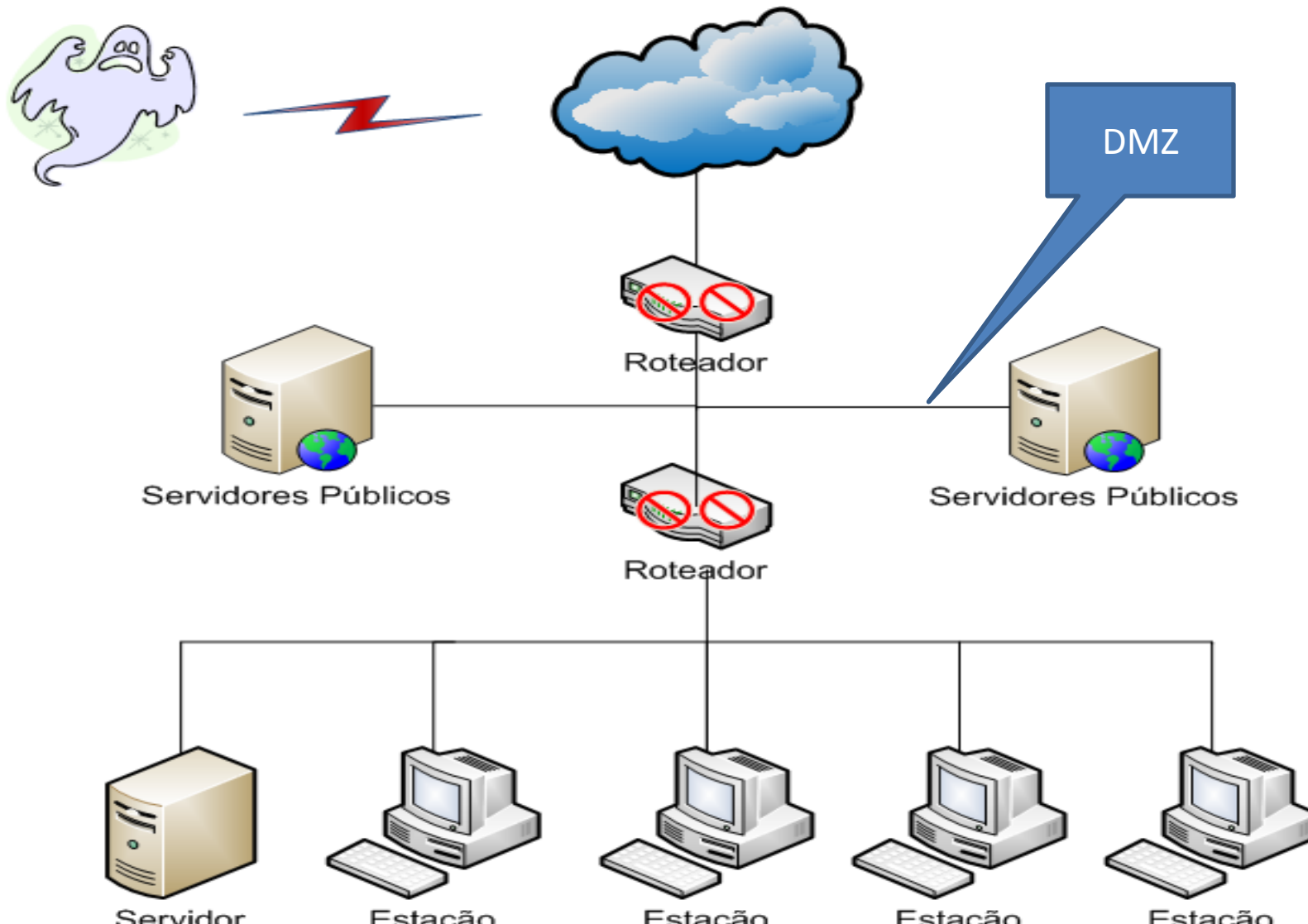
Firewalls – Arquitetura simples



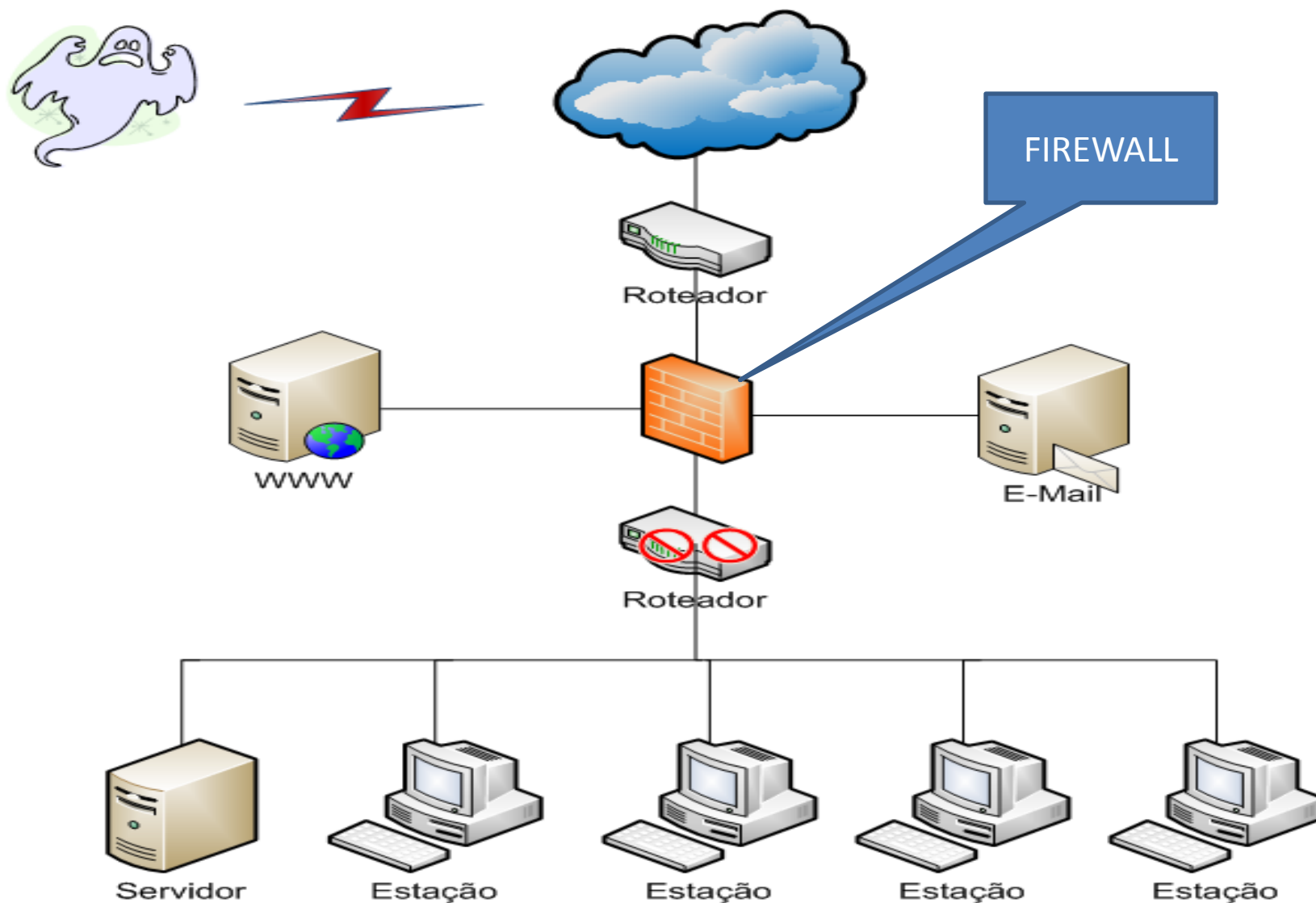
Firewalls – Arquitetura Bastion Host



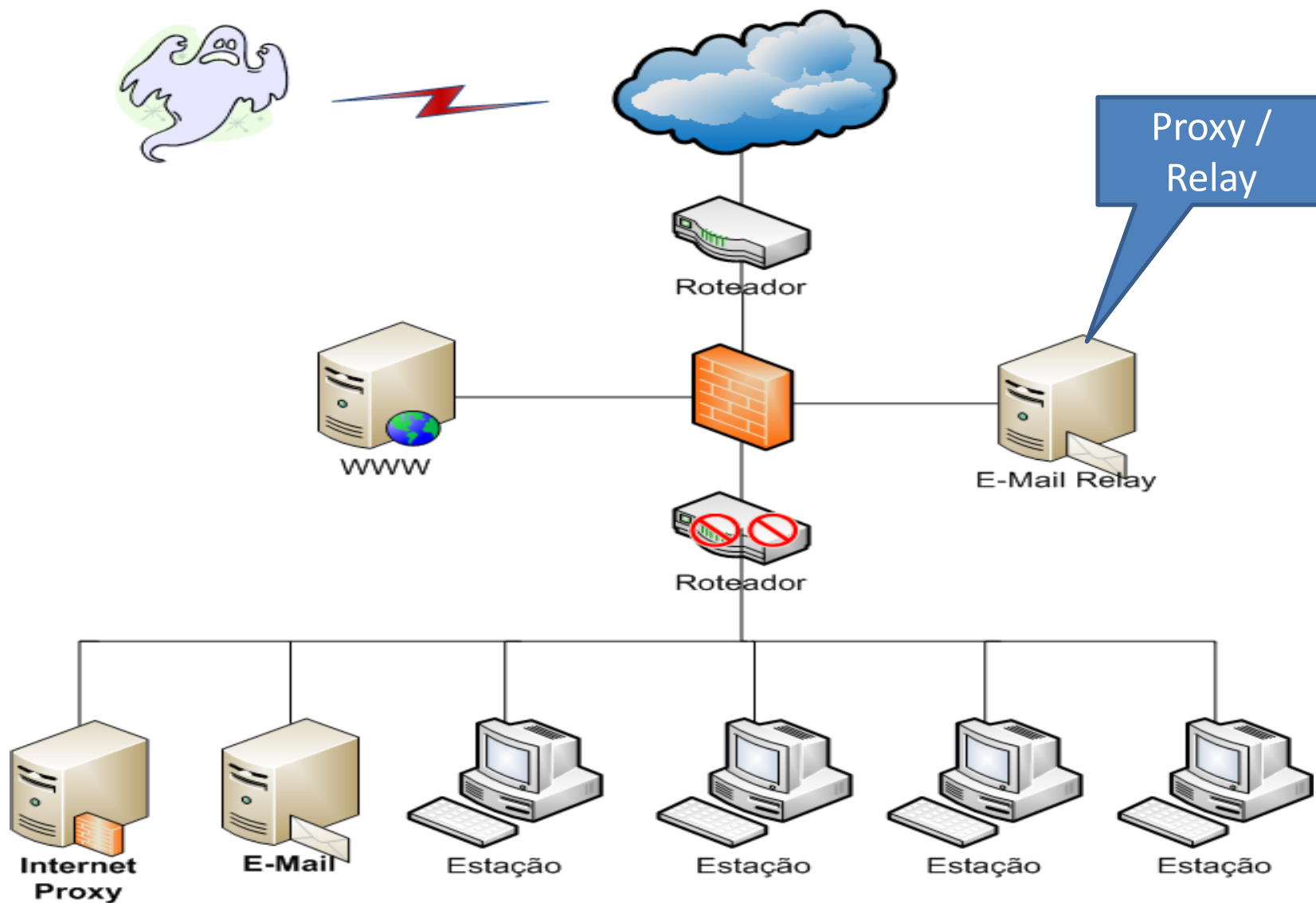
Firewalls – Arquitetura DMZ



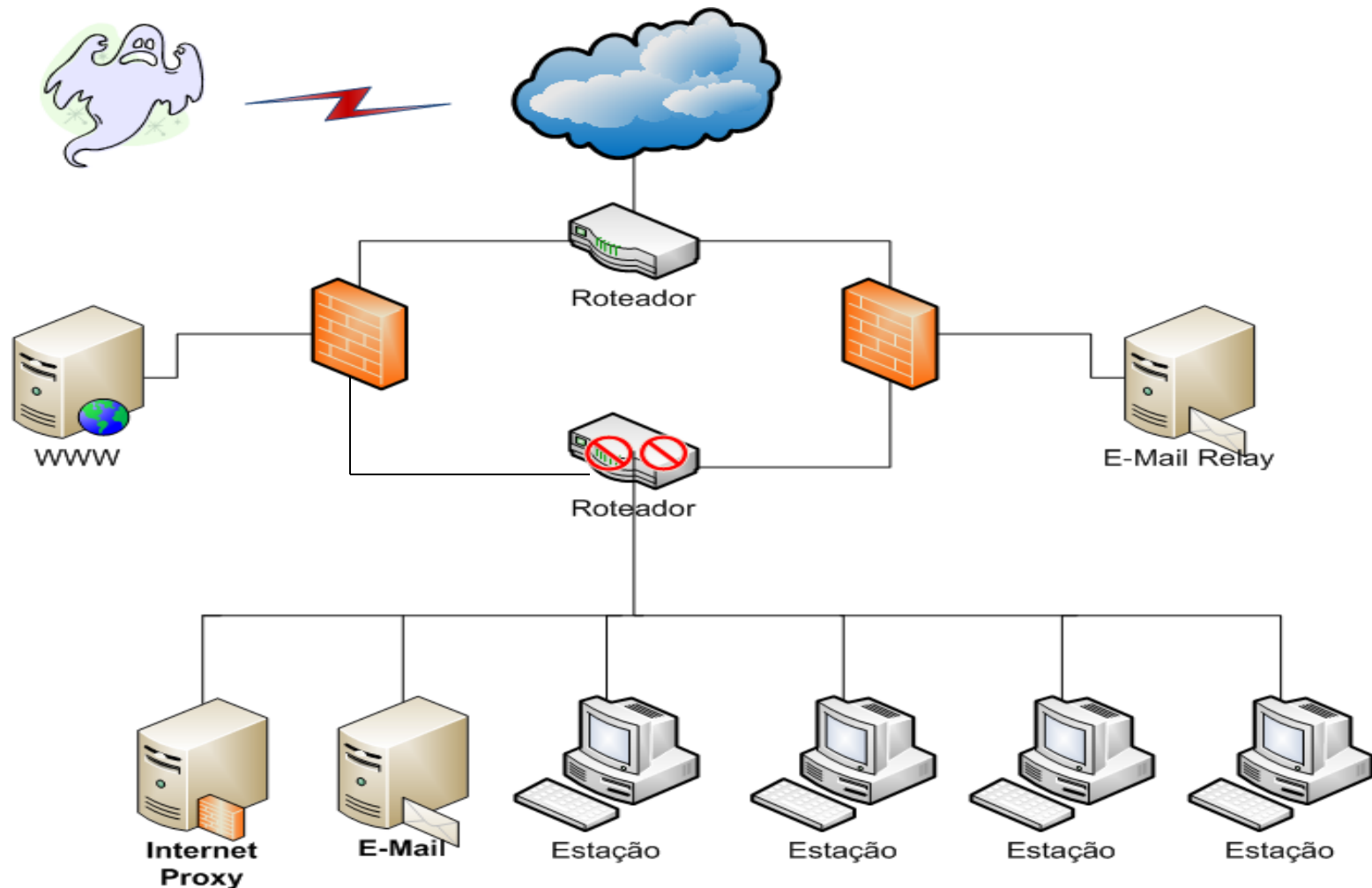
Firewalls – Arquitetura com FW



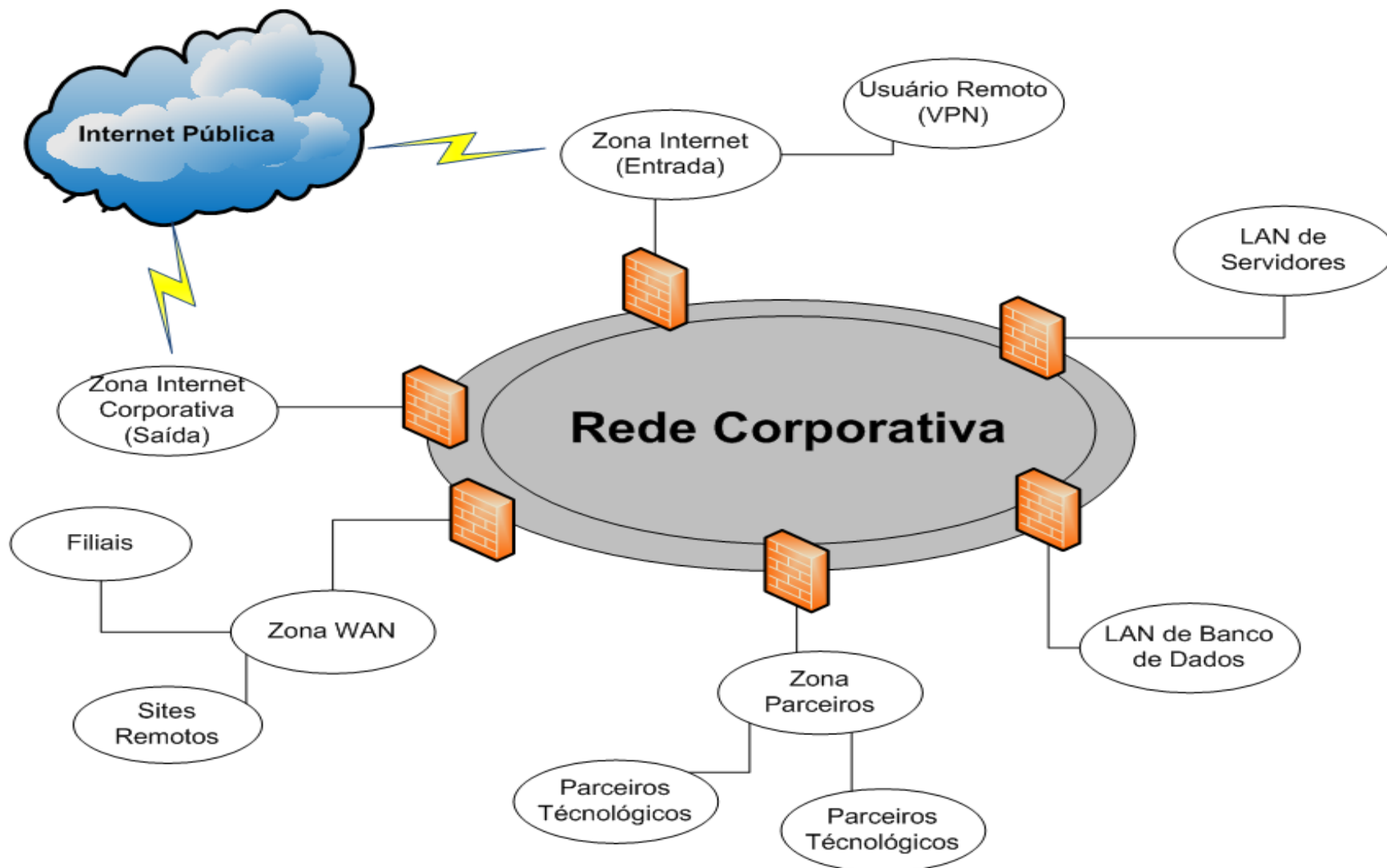
Firewalls – Arquitetura Relay



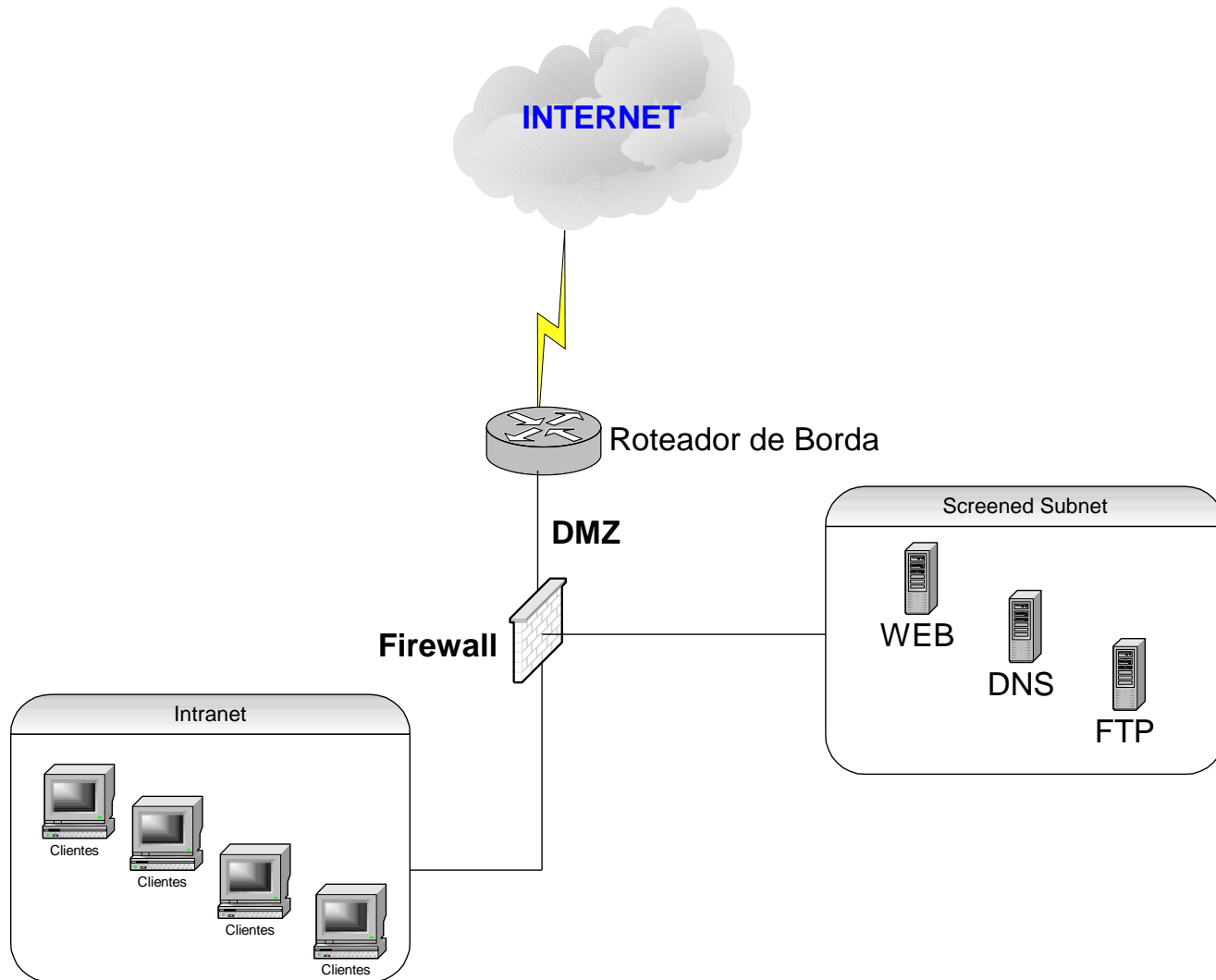
Firewalls – Camadas de Relay



Firewalls – Segregação de Redes



Firewalls – Ambiente



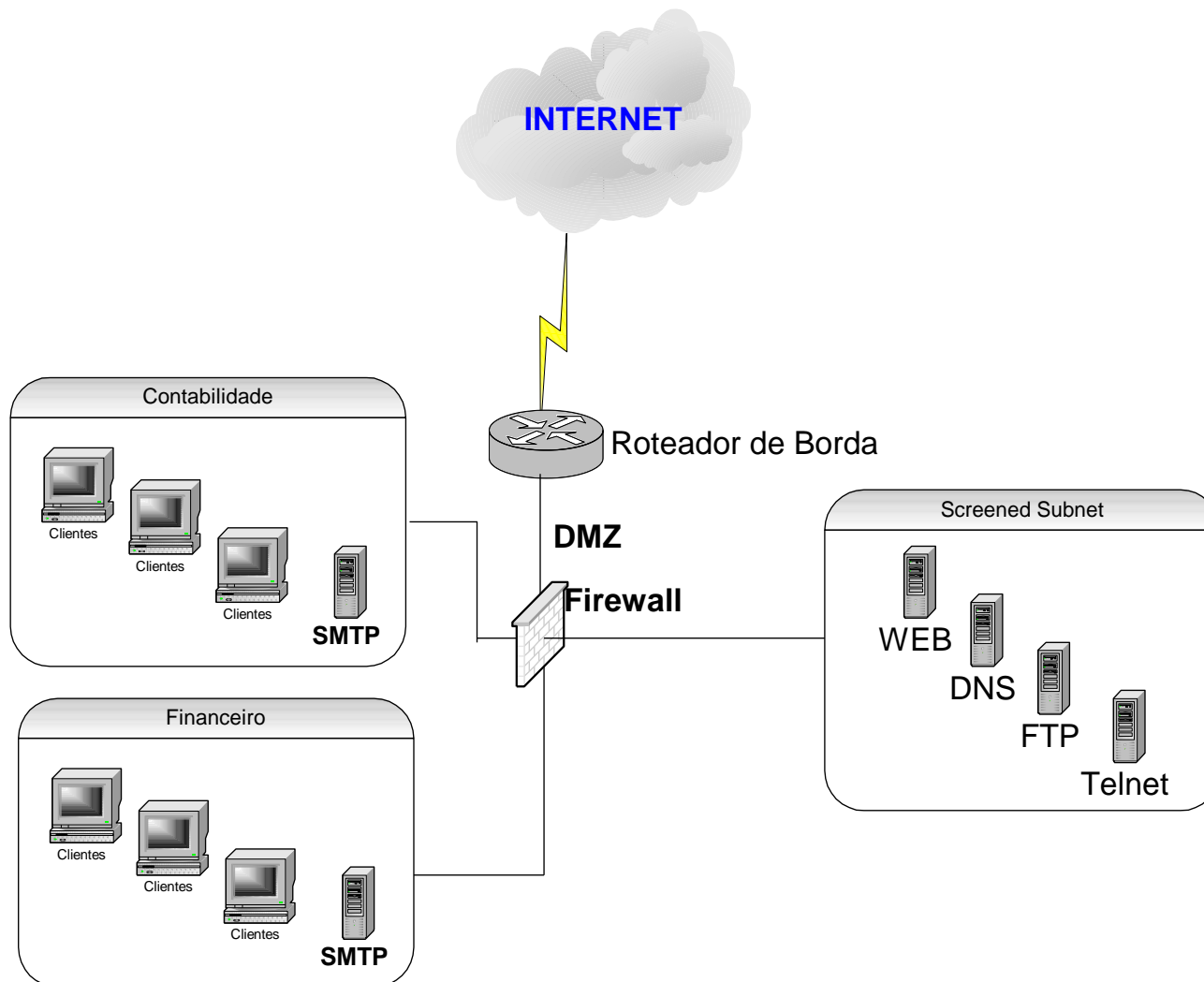
Firewalls – Ambiente

Origem	Destino	Protocolo	Porta (O)	Porta (D)	Ação	Horário
*	200.200.200.200	tcp	*	80	Aceita	*
200.200.1.1	200.200.200.201	tcp	*	21	Aceita	*
*	*	tcp/udp	*	53	Aceita	*
10.10.10.0	*	tcp	*	*	Aceita	Comercial
10.10.10.0	*	udp	*	*	Aceita	*
*	*	*	*	*	<i>Nega</i>	*

Firewalls – Exercício Prático

- Defina uma política de Firewall para o ambiente proposto, tendo em vista as premissas determinadas, utilize como exemplo as tabelas e campos determinados anteriormente.
- Escolha a melhor estratégia e determine a política mais simples possível.

Firewalls – Exercício Prático



Firewalls – Exercício Prático

- Simular a criação de uma política, levando em consideração as informações aqui fornecidas, lembrando que algumas delas podem ser implícitas ou não foram claramente definidas, como ocorre na vida real, nesse caso a implantação das políticas de Firewall só poderá ser concretizada após sabada todas as dúvidas com relação ao ambiente.

Firewalls – Exercício Prático

- Endereçamento

Objeto	Endereço
Rede Contabilidade	10.10.10.0 / 24
Rede Financeiro	10.10.20.0 / 24
DNS	200.200.200.1
FTP	200.200.200.2
Telnet	200.200.200.3
Web	200.200.200.4

- As redes Contabilidade e Financeiro podem trocar arquivos e e-mails entre si. Os arquivos só devem ser trocados via FTP.
- Contabilidade pode acessar tudo na Internet.
- Financeiro somente páginas Web

Firewalls – Exercício Prático

- As redes Contabilidade e Financeiro devem estar protegidas da Internet.
- Contabilidade e Financeiro não poderão enviar e-mail para a Internet.
- As máquinas publicadas na Internet não poderão disponibilizar outros serviços que não os configurados.
- O Servidor de telnet só poderá ser acessado pela rede Contabilidade e Financeiro.