UNIVERSIDADE
EDUARDO
MONDLANE

FACULDADE DE ENGENHARIA
DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA
LICENCIATURA EM ENGENHARIA INFORMÁTICA
REDES DE COMPUTADORES I

TEMA: Mecanismos de Segurança de Sistemas de Informação

Grupo Docente:

- **:** Engº. Ivone Cipriano
- **:** Engº. Délcio Chadreca

Tópicos da Aula

- Introducao
- Firewalls de Pacotes
- Firewalls de Aplicação
- Firewalls de Estado
- Firewalls baseados em Nuvem
- Firewalls de Software
- Firewalls de Hardware
- Firewalls de Próxima Geração
- IDS e IPS
- SIEM
- Configuracao de Firewall

Introdução

Mecanismos de segurança de sistemas de informação são ferramentas, tecnologias e práticas que visam proteger os sistemas de informação de uma organização contra ameaças cibernéticas, como hackers, vírus, malware e outras formas de ataques cibernéticos.

Esses mecanismos ajudam a garantir a confidencialidade, integridade e disponibilidade dos dados, bem como a continuidade dos negócios.

Mecanismos de segurança de sistemas de informação

- Sistemas de prevenção de intrusão (IPS): uma tecnologia de segurança que detecta e impede ataques cibernéticos em tempo real.
- Autenticação multifactorial (MFA): um método de autenticação que requer mais de uma forma de autenticação (como senha e token de segurança) para acessar um sistema.
- Criptografia: um método para proteger dados em trânsito ou armazenados, transformando-os em um formato ilegível para aqueles que não possuem a chave de criptografia.

Cont.

- Firewall: um dispositivo de segurança de rede que controla o tráfego de rede com base em regras predefinidas.
- Antivírus: um software de segurança que detecta e remove vírus e malware de sistemas de computador.
- Sistemas de detecção de intrusão (IDS): uma tecnologia de segurança que monitora a rede ou os sistemas de computador em busca de actividades suspeitas ou anómalas que possam indicar uma violação de segurança.

Firewalls

Firewalls são sistemas de segurança de rede que controlam o tráfego de rede com base em regras de segurança predefinidas.

Eles são projectados para proteger redes e sistemas de computadores de ameaças cibernéticas, como ataques de hackers, malware e outras formas de ataques cibernéticos.

Um Firewall não é uma máquina, é uma infra-estrutura mais ou menos complexa que isola um perímetro protegido de redes perigosas a que o mesmo se liga.

Firewalls de Pacotes

Firewalls de Pacotes são um dos tipos mais antigos e simples de Firewall. Eles operam na camada de rede do modelo OSI (Open Systems Interconnection) e analisam cada pacote de dados que entra ou sai da rede para decidir se permitir ou bloquear com base em regras pré-determinadas.

Os Firewalls de Pacotes são eficazes em bloquear tráfego indesejado, como conexões externas não solicitadas e pacotes de dados malformados ou inválidos.

No entanto, eles têm algumas limitações. Por exemplo, eles não podem examinar o conteúdo do pacote de dados, o que significa que não podem identificar ameaças que estejam ocultas dentro de um pacote de dados válido.

Firewalls de Aplicação

Firewalls de Aplicação (também conhecidos como Firewalls de Camada de Aplicação ou WAFs - Web Application Firewalls) são projectados para proteger aplicativos específicos, analisando o conteúdo de cada pacote de dados que entra ou sai do aplicativo.

Eles operam na camada de aplicação do modelo OSI e podem filtrar o tráfego com base em regras pré-determinadas ou em comportamentos conhecidos de ataques.

Os Firewalls de Aplicação são particularmente úteis na protecção de aplicativos web, que são vulneráveis a uma ampla variedade de ataques, como injecção SQL, XSS (Cross-Site Scripting) e CSRF (Cross-Site Request Forgery).Eles são capazes de identificar esses tipos de ataques e bloquear o tráfego malicioso antes que chegue ao aplicativo.

Cont.

Os Firewalls de Aplicação também podem inspeccionar o conteúdo do tráfego de rede para garantir que ele esteja em conformidade com as políticas de segurança da rede. Por exemplo, eles podem bloquear tráfego que contenha informações confidenciais ou senhas em texto claro.

Embora os Firewalls de Aplicação ofereçam uma camada adicional de protecção para aplicativos específicos, eles não são uma solução completa para a segurança de rede. Eles não podem proteger contra ataques em outras camadas do modelo OSI e podem ser contornados por ataques sofisticados que tentam evitá-los.

No geral, os Firewalls de Aplicação são uma ferramenta importante na estratégia de segurança de rede, especialmente para organizações que dependem de aplicativos web críticos para os negócios. Eles podem ser usados em conjunto com outros tipos de Firewall e medidas de segurança para garantir a proteção completa da rede.

Firewalls de Estado

Firewalls de Estado (também conhecidos como Firewalls de Camada de Transporte) são projectados para monitorar o estado das conexões de rede e tomar decisões de filtragem de pacotes com base no estado da conexão.

Eles operam na camada de transporte do modelo OSI e são capazes de filtrar o tráfego com base em informações do cabeçalho do pacote, como o endereço de origem e destino, o protocolo de transporte e o número de porta.

Os Firewalls de Estado são capazes de examinar todo o fluxo de tráfego em uma conexão de rede, em vez de apenas pacotes individuais, o que lhes permite tomar decisões de filtragem mais inteligentes. Eles podem “lembrar” o estado de cada conexão e permitir ou bloquear o tráfego com base em regras de política pré-determinadas.

Cont.

Os Firewalls de Estado também são capazes de detectar e bloquear tentativas de conexões maliciosas, como conexões de ataque DoS (Denial-of-Service) e SYN flooding. Além disso, eles podem bloquear conexões que estão em desacordo com as políticas de segurança da rede, como conexões de origem desconhecida ou tráfego de porta não autorizado.

Os Firewalls de Estado são geralmente considerados uma opção mais avançada do que os Firewalls de Pacotes, mas menos avançados do que os Firewalls de Aplicação. Eles são uma solução de segurança de rede muito comum e amplamente utilizada em todo o mundo.

No geral, os Firewalls de Estado são uma parte importante de uma estratégia de segurança de rede completa e podem ser usados em conjunto com outros tipos de Firewall para fornecer protecção abrangente da rede.

Firewalls baseados em Nuvem

Firewalls baseados em Nuvem são uma opção relativamente nova em termos de segurança de rede e estão ganhando popularidade devido à sua flexibilidade, escalabilidade e eficácia.

Esses Firewalls são executados em nuvens públicas ou privadas e são geridos remotamente, fornecendo uma camada de segurança de rede em qualquer lugar em que a organização tenha conectividade com a internet.

Os Firewalls baseados em Nuvem funcionam da mesma forma que os Firewalls de Hardware ou de Software tradicionais, filtrando o tráfego de rede com base em regras de política.

No entanto, eles oferecem uma série de vantagens adicionais. Em primeiro lugar, eles são altamente escaláveis, permitindo que as organizações ajustem a capacidade do Firewall de acordo com as necessidades de sua rede. Isso significa que as organizações podem evitar a necessidade de investir em hardware adicional para expandir sua capacidade de Firewall.

Cont.

Em segundo lugar, os Firewalls baseados em Nuvem podem ser facilmente gerenciados remotamente, permitindo que as organizações gerenciem sua segurança de rede a partir de qualquer lugar com conectividade com a internet. Isso é particularmente útil para organizações que têm vários escritórios ou que permitem que seus funcionários trabalhem remotamente.

Além disso, os Firewalls baseados em Nuvem podem oferecer uma protecção mais eficaz contra ameaças de segurança cibernética, como ataques DDoS, graças à sua capacidade de distribuir o tráfego de rede por vários servidores em nuvem.

No entanto, os Firewalls baseados em Nuvem também apresentam algumas desvantagens, como a dependência da conectividade com a internet e a possibilidade de latência na rede. Além disso, a segurança da nuvem em que o Firewall está sendo executado deve ser cuidadosamente avaliada para garantir que ela atenda aos padrões de segurança e privacidade da organização.

Firewalls de Software

Firewalls de Software são programas de segurança de rede que podem ser instalados em computadores e servidores. Eles são projectados para monitorar o tráfego de rede e filtrar pacotes de dados suspeitos com base em regras de política pré-determinadas.

Os Firewalls de Software são capazes de monitorar o tráfego de rede em tempo real e podem ser configurados para permitir ou bloquear o acesso a recursos de rede com base em critérios como endereço IP, protocolo e porta. Eles também podem ser configurados para permitir ou bloquear determinados tipos de tráfego de rede, como tráfego de e-mail ou tráfego da web.

Os Firewalls de Software são uma opção económica para empresas que desejam implementar uma solução de segurança de rede eficaz sem a necessidade de investir em hardware dedicado. Eles podem ser facilmente instalados em computadores e servidores e são fáceis de configurar e gerenciar.

Cont.

Os Firewalls de Software também podem ser integrados com outros sistemas de segurança, como antivírus e prevenção de intrusões, para fornecer protecção abrangente da rede. Eles também podem ser actualizados com facilidade, permitindo que as organizações se adaptem às ameaças emergentes e garantam a segurança contínua da rede.

No entanto, os Firewalls de Software têm algumas limitações em comparação com os Firewalls de Hardware. Eles podem ser menos eficazes em lidar com grandes volumes de tráfego de rede e podem ser mais susceptíveis a ataques de hackers e malware. Além disso, como eles são instalados em computadores e servidores, eles podem afectar o desempenho do sistema, especialmente em ambientes de rede de alta carga.

Firewalls de Hardware

Firewalls de Hardware são dispositivos físicos projetados especificamente para fornecer segurança de rede. Eles são construídos para operar como uma camada de defesa externa para a rede, protegendo-a contra ameaças externas, como ataques de hackers e malware.

Os Firewalls de Hardware são projectados para processar o tráfego de rede em tempo real, filtrando e bloqueando pacotes de dados suspeitos. Eles geralmente incluem múltiplas portas de rede, permitindo que o tráfego de entrada e saída da rede seja monitorado e filtrado de forma eficaz. Alguns Firewalls de Hardware também incluem recursos de balanceamento de carga, que permitem que o tráfego seja distribuído uniformemente entre várias conexões de rede.

Cont.

Os Firewalls de Hardware podem ser instalados em qualquer lugar na rede, incluindo na borda da rede, onde ela se conecta à internet. Eles podem ser configurados para aplicar políticas de segurança de rede consistentes em toda a organização, o que ajuda a garantir a conformidade com as regulamentações de segurança e privacidade.

Os Firewalls de Hardware também são considerados uma opção mais segura do que os Firewalls de Software, uma vez que estão fisicamente separados da rede e são menos susceptíveis a ataques de hackers e malware. Além disso, os Firewalls de Hardware podem ser actualizados com facilidade, permitindo que as organizações se adaptem às ameaças de segurança emergentes e garantam a segurança contínua da rede.

Cont.

No geral, os Firewalls de Hardware são uma parte importante de uma estratégia de segurança de rede completa e são amplamente utilizados em organizações de todos os tamanhos e sectores. Eles fornecem uma camada de segurança física e confiável que protege a rede contra ameaças externas e mantém a organização segura e protegida.

Firewalls de Próxima Geração

Firewalls de Próxima Geração (NGFW - Next-Generation Firewalls) são a evolução dos Firewalls tradicionais e são projectados para fornecer uma camada de segurança mais avançada e abrangente. Eles são capazes de realizar análises mais profundas do tráfego de rede em tempo real, utilizando tecnologias como análise comportamental, inspecção SSL, prevenção de intrusões e filtragem de conteúdo.

Os NGFWs operam em várias camadas do modelo OSI, incluindo a camada de aplicação, camada de transporte e camada de rede. Eles são capazes de examinar o conteúdo do tráfego em tempo real e tomar decisões de filtragem com base em regras de política pré-determinadas e análises avançadas.

Cont.

Os Firewalls de Próxima Geração são capazes de identificar e bloquear ameaças sofisticadas, como malware avançado e ataques de dia zero.

Eles também podem identificar e bloquear tráfego malicioso que se disfarça como tráfego legítimo e podem proteger contra ataques de engenharia social, como phishing e spear-phishing.

Os NGFWs também incluem recursos de controle de acesso, que permitem que os administradores de rede restrinjam o acesso a determinados recursos de rede com base em funções de usuário ou outros critérios.

Eles também podem monitorar o tráfego de rede para detectar e prevenir comportamentos suspeitos, como tentativas de acessar recursos de rede não autorizados.

Resumo

Os Firewalls de Próxima Geração fornecem uma camada de segurança avançada e abrangente para redes corporativas, permitindo que as organizações monitorem e protejam suas redes contra ameaças conhecidas e desconhecidas.

Eles são uma parte fundamental de uma estratégia de segurança de rede completa e podem ser usados em conjunto com outros tipos de Firewall e soluções de segurança para fornecer proteção abrangente da rede.

Intrusion Detection System - IDS

Os Sistemas de Detecção de Intrusão (IDS, do inglês Intrusion Detection System) são ferramentas de segurança cibernética que monitoram e analisam o tráfego de rede em busca de atividades maliciosas ou comportamentos anômalos que possam indicar uma tentativa de invasão ou violação de segurança.

Existem dois tipos principais de IDS: IDS de Rede e IDS de Host.

- O IDS de Rede monitora o tráfego de rede em busca de padrões de tráfego malicioso ou suspeito e alerta o administrador de segurança quando é detectada uma atividade potencialmente maliciosa.
- Já o IDS de Host é instalado em um sistema operacional de um host específico para monitorar as atividades no host e identificar possíveis atividades maliciosas.

Cont.

existem duas abordagens diferentes para detectar intrusões:

- A primeira é baseada em assinaturas, que envolve a comparação do tráfego de rede ou atividade do host com uma base de dados de assinaturas de ataques conhecidos.
- A segunda é baseada em comportamento, que envolve a análise do tráfego de rede ou atividade do host em busca de comportamentos anômalos que possam indicar uma atividade maliciosa.

Os IDS podem ser implementados como hardware ou software e podem ser configurados para enviar alertas para um administrador de segurança ou tomar medidas automatizadas para bloquear o tráfego malicioso.

Os IDS são frequentemente usados em conjunto com outros controles de segurança, como Firewalls e Sistemas de Prevenção de Intrusões (IPS, do inglês Intrusion Prevention System), para fornecer uma camada adicional de proteção contra ameaças cibernéticas.

Intrusion Prevention System- IPS

Os Sistemas de Prevenção de Intrusão (IPS, do inglês Intrusion Prevention System) são uma tecnologia de segurança cibernética que monitora o tráfego de rede em tempo real para detectar e bloquear actividades maliciosas. Eles são uma evolução dos Sistemas de Detecção de Intrusão (IDS) e, ao contrário dos IDS, podem tomar medidas activas para prevenir o tráfego malicioso em vez de apenas alertar o administrador de segurança.

Existem dois tipos principais de IPS:

- O IPS de rede, que é implementado como um dispositivo de segurança em uma rede e monitora o tráfego de rede em busca de actividades maliciosas. Quando uma actividade maliciosa é detectada, o IPS pode tomar medidas activas para bloquear o tráfego malicioso.
- O IPS de host, que é instalado em um sistema operacional de um host específico e monitora as actividades no host para detectar actividades maliciosas. O IPS de host pode tomar medidas ativas para bloquear a actividade maliciosa ou alertar o administrador de segurança.

Cont.

O IPS pode ser baseado em assinaturas ou comportamento, assim como o IDS. A tecnologia baseada em assinaturas compara o tráfego de rede ou actividade do host com uma base de dados de assinaturas de ataques conhecidos. Já a tecnologia baseada em comportamento envolve a análise do tráfego de rede ou actividade do host em busca de comportamentos anómalos que possam indicar uma actividade maliciosa.

Os IPS são uma importante ferramenta de segurança cibernética que ajudam a proteger as redes e sistemas contra ameaças cibernéticas. Eles podem ser usados em conjunto com outros controles de segurança, como firewalls e sistemas de detecção de intrusão, para fornecer uma camada adicional de protecção contra ameaças cibernéticas.

Security Information and Event Management - SIEM

SIEM (Security Information and Event Management) é uma tecnologia de segurança cibernética que combina a capacidade de colectar e analisar dados de segurança de vários dispositivos e sistemas em uma única plataforma centralizada. A tecnologia SIEM ajuda as organizações a detectar, investigar e responder a ameaças cibernéticas em tempo real.

O SIEM funciona colectando dados de segurança de vários dispositivos, como firewalls, sistemas de detecção de intrusão, sistemas de prevenção de intrusão, servidores, roteadores e outros dispositivos de rede. Esses dados são colectados em um único repositório centralizado, onde são analisados e correlacionados para identificar actividades suspeitas ou anómalas que possam indicar uma ameaça cibernética.

Cont.

O SIEM usa algoritmos de análise de dados para identificar e correlacionar eventos de segurança em diferentes dispositivos e sistemas. Ele também pode usar técnicas de machine learning e inteligência artificial para melhorar a precisão da análise e identificar padrões de comportamento que possam indicar ameaças cibernéticas.

Os sistemas SIEM também podem incluir recursos de gerenciamento de incidentes, permitindo que as equipes de segurança priorizem e investiguem as ameaças cibernéticas com mais eficiência. Alguns sistemas SIEM podem até mesmo fornecer recursos de automação, permitindo que as equipes de segurança executem ações corretivas em tempo real.

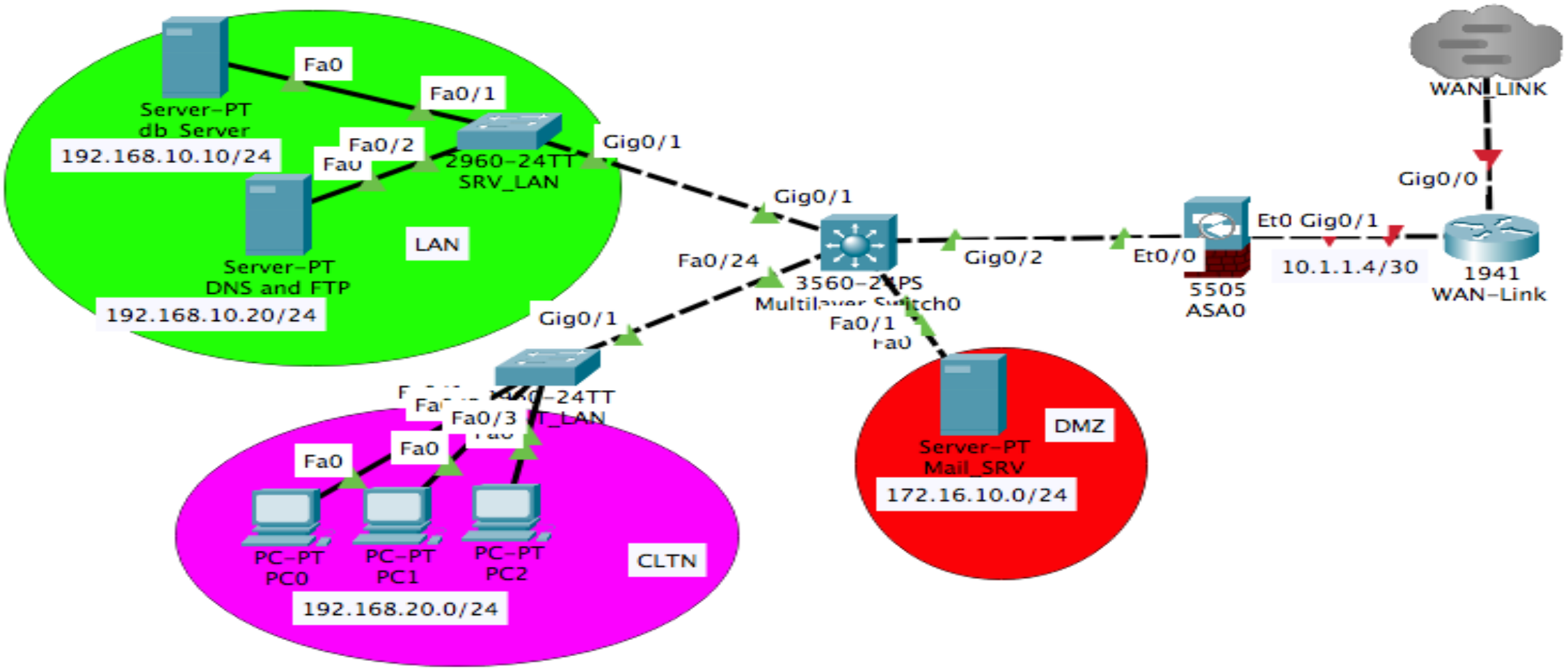
Politicas de Firewalls

Uma Politica de Firewall é implementada num firewall através de regras. A maior parte da administração de um Firewall consiste na configuração de regras como as que seguem:

- Permitir que todos os IPs internos possam aceder à Web
- Permitir todo o tráfego de e-mail a partir do servidor interno
- Efectuar *drop* a todo o tráfego que não obedeça a nenhuma das duas regras anteriores
- Permitir tráfego do exterior que se destina ao servidor Web publico
- Efectuar *drop* a todo o tráfego proveniente do exterior, a menos que seja destinado ao servidor *web* publico
- Registar todas as tentativas de ligação que sejam rejeitadas pelo firewall
- Registar todos os acessos a servidores *web* externos

As regras tem de cobrir o conjunto de acções para pacotes da rede interna e tentam sair para a rede externa, bem como para pacotes da rede exterior que tentam alcançar a rede interna.

Principio Básico de Configuração do Firewall



PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO

Firewalls

Exemplo da Aplicação de Firewalls

Para explicar como são construídas e usadas as regras (Política de Firewalls) vamos considerar a abaixo esquematizada:

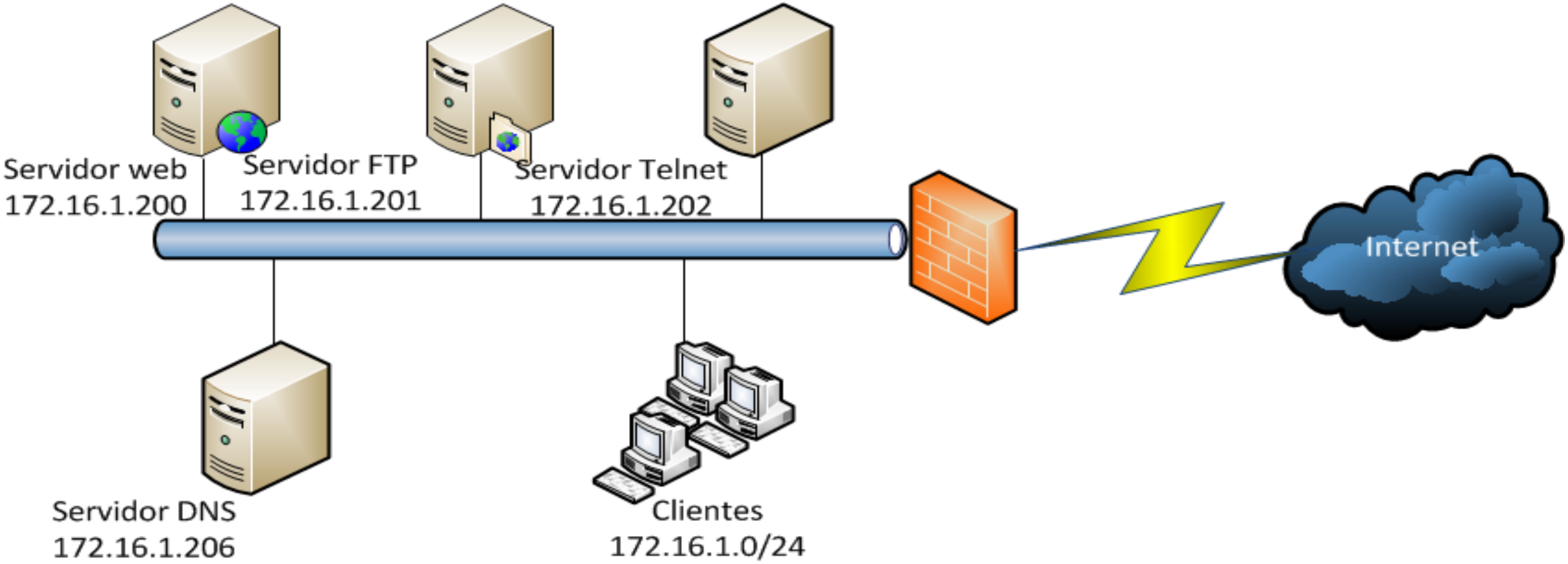


Tabela 5.1-Regras para serviço web do exterior para o interno

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
HTTP	TCP	Qualquer	Qualquer	172.16.1.200	80	Permite
HTTPS	TCP	Qualquer	Qualquer	172.16.1.200	443	Permite

Tabela 5.2-Regras para serviço *web* do interior para *o* exterior

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
HTTP	TCP	172.16.1.0/24	Qualquer	Qualquer	80	Permite
HTTPS	TCP	172.16.1.0/24	Qualquer	Qualquer	443	Permite

Tabela 5.3-Regras para utilização do DNS interno

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
DNS	TCP	Qualquer	Qualquer	172.16.1.206	53	Permite
DNS	UDP	Qualquer	Qualquer	172.16.1.206	53	Permite

Tabela 5.4-Regras para consulta a servidores DNS no exterior

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
DNS	TCP	172.16.1.206	Qualquer	Qualquer	53	Permite
DNS	UDP	172.16.1.206	Qualquer	Qualquer	53	Permite

Tabela 5.5-Regras para reencaminhamento de DNS aos servidores do ISP

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
DNS	TCP	172.16.1.206	Qualquer	39.200.12.65	53	Permite
DNS	UDP	172.16.1.206	Qualquer	39.200.12.65	53	Permite

Tabela 5.6-Regras para a ligação de cliente externo ao sevidor FTP interno

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
FTP	TCP	Qualquer	Qualquer	172.16.1.201	21	Permite
FTP (dados)	TCP	172.16.1.201	20	Qualquer	Qualquer	Permite
FTP (passivo)	TCP	Qualquer	Qualquer	172.16.1.201	Qualquer	Permite

Tabela 5.7-Regras para a ligação de cliente interno ao sevidor FTP externo

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
FTP	TCP	172.16.1.0/24	Qualquer	Qualquer	21	Permite
FTP (dados)	TCP	Qualquer	20	172.16.1.0/24	Qualquer	Permite

Tabela 5.8-Regras para a utilização do Microsoft Messenger

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
IM	TCP	Qualquer	Qualquer	Qualquer	1863	Permite
HTTP	TCP	Qualquer	Qualquer	Qualquer	80	Permite

Tabela 5.9-Regras para transferência de ficheiros com Microsoft Messenger

PROTOCOLO	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
File Transfer (P/interior)	Qualquer	Qualquer	IP do destinatário	6891 - 6900	Permite
File Transfer (P/exterior)	172.16.1.0/24	Qualquer	IP do destinatário	6891 - 6900	Permite

Tabela 5.10-Regra para permitir utilização de serviço IRC (*Internet Relay Chat*)

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
IRC	TCP	Qualquer	Qualquer	Qualquer	6667	Permite

Tabela 5.11-Regra para permitir Telnet ao servidor interno

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
Telnet	TCP	Qualquer	Qualquer	172.16.1.202	23	Permite

Tabela 5.12-Regra para permitir Telnet ao servidores externos

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
Telnet	TCP	172.16.1.0/24	Qualquer	Qualquer	23	Permite

Tabela 5.13-Regras para permitir correio electrónico para o exterior

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
POP3	TCP	172.16.1.0/24	Qualquer	Qualquer	110	Permite
POP3/S	TCP	172.16.1.0/24	Qualquer	Qualquer	995	Permite
IMAP	TCP	172.16.1.0/24	Qualquer	Qualquer	143	Permite
IMAP/S	TCP	172.16.1.0/24	Qualquer	Qualquer	993	Permite
SMTP	TCP	172.16.1.0/24	Qualquer	Qualquer	25	Permite
SMTP/S	TCP	172.16.1.0/24	Qualquer	Qualquer	465	Permite
HTTP	TCP	172.16.1.0/24	Qualquer	Qualquer	80	Permite
HTTPS	TCP	172.16.1.0/24	Qualquer	Qualquer	443	Permite
LDAP	TCP	172.16.1.0/24	Qualquer	Qualquer	389	Permite
LDAPS	TCP	172.16.1.0/24	Qualquer	Qualquer	636	Permite

Tabela 5.14-Regras para permitir acesso ao servidor interno de correio electrónico

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
POP3	TCP	Qualquer	Qualquer	172.16.1.210	110	Permite
POP3/S	TCP	Qualquer	Qualquer	172.16.1.210	995	Permite
IMAP	TCP	Qualquer	Qualquer	172.16.1.210	143	Permite
IMAP/S	TCP	Qualquer	Qualquer	172.16.1.210	993	Permite
SMTP	TCP	Qualquer	Qualquer	172.16.1.210	25	Permite
SMTP/S	TCP	Qualquer	Qualquer	172.16.1.210	465	Permite
HTTP	TCP	Qualquer	Qualquer	172.16.1.210	80	Permite
HTTPS	TCP	Qualquer	Qualquer	172.16.1.210	443	Permite
LDAP	TCP	Qualquer	Qualquer	172.16.1.210	389	Permite
LDAPS	TCP	Qualquer	Qualquer	172.16.1.210	636	Permite

PROTOCOLO	TRANSPORTE	IP ORIGEN	PORTA ORIGEN	IP DESTINO	PORTA DESTINO	ACÇÃO
Qualquer	Qualquer	Qualquer	Qualquer	Qualquer	Qualquer	Destrói

Como as regras de um firewall funcionam em cascata, se a analise do pacote não for apanhada por nenhuma regra, então esta ultima regra procede à destruição do mesmo, evitando que alcance a rede protegida

Desafios de selecção de Firewalls

Desafios da Gestão e administração de firewall

OBRIGADO !!!