Insper

Roteiro Gateway de aplicação - Proxy

Objetivo: A criação de um servidor de filtragem de acesso Internet configurado para atender uma política de segurança.

Introdução

O Termo “servidor proxy”, vem de uma palavra em inglês que significa procuração. Este aplicativo também pode ser conhecido como gateway de aplicação, entretanto ficando limitado apenas a alguns protocolos como http, https e ftp. Hoje o proxy tem a grande vantagem de atuar como um cache de páginas web. Se você abre, por exemplo o site www.rodolfoavelino.com.br, na segunda vez que acessá-lo, tudo que estiver armazenado no espaço em disco do proxy será enviado ao seu browser sem que o proxy tenha feito um novo download na internet, economizando tempo e banda de internet.

As requisições de sites são feitas das estações através do proxy, ou seja, o proxy, é o responsável em realizar a busca e entrega do site para o usuário.

Por meio da criação de Acls é possível o cadastro de sites e servidores comprometidos permitindo assim que um usuário desatento acesse um link malicioso.

Exemplos de ACLs

src: Tipo utilizado para indicar endereços IP de origem. Pode-se especificar um endereço de rede, como 192.168.16.0/24, um endereço de um determinado *host*, como 192.168.16.10/24 ou uma faixa de endereços, como 192.168.16.10-192.168.16.20/24

Exemplos:

acl rede_local src 192.168.1.0/255.255.255.0

acl recepcao src 192.168.1.15

dst: Utilizada para especificar um determinado host ou rede de destino.

Exemplo:

acl rede_local dst 192.168.1.0/255.255.255.0

Insper

dstdomain: Utilizado para especificar um determinado domínio de destino.

Exemplo:

acl facebook dstdomain .facebook.com

url_regex: Este tipo percorre a URL a procura da expressão regular especificada. Deve ser observado que a expressão é *case-sensitive*, para que seja *case-insensitive* deve ser usada a opção -i. É o tipo mais comum de ACL dada a flexibilidade proporcionada pelo uso de expressões regulares.

Exemplos:

acl bloqueios url_regex -i **jogos pedofilia pornografia**

Caso a lista de bloqueios seja grande você pode optar em criar uma lista e declarar o caminho absoluto do arquivo conforme acl abaixo:

acl bloqueios url_regex -i "/etc/squid/palavras_proibidas"

dstdomain_regex: Procura por expressão no domínio. Usado da mesma forma que *srcdom_regex*, entretanto com relação ao destino.

Exemplo:

acl sites_proibidos dstdomain_regex -i "/etc/squid/sites_proibidos"

Exercício 1: Altere a porta padrão do serviço para a porta 8088

Exercício 2: Limpe o arquivo de configuração

Exercício 3: Criação de Lista de controle de acessos. Crie a política de acesso da rede seguindo os itens abaixo. Você poderá atribuir os números Ips livremente de acordo com a configuração de endereçamento de sua rede. Por favor listar os endereços para os seguintes hosts:

Recepção:

Insper

Gerencia:

a) Nenhuma máquina da rede deverá realizar downloads de arquivos com as seguintes extensões: .src , .exe, .paf, .mp3, .mp4.

b) A máquina da gerência deverá ter acesso irrestrito a sites.

c) Os domínios twitter.com e youtube.com deverão ser bloqueados.

d) sites que contenham a palavra terra deverão ser bloqueados, contudo o site terraviva.com.br deverá estar disponível para o acesso.

e) O host da recepção deverá apenas acessar o site terraviva.com.br.

Exercício 4: Instalar e disponibilizar uma ferramenta para a geração de relatórios de acessos a páginas de sua rede (Enviar o print de um relatório gerado).

Orientações: Você deverá depositar o arquivo squid.conf no blackboard até 16/05/2024.

Bibliografia e dicas para consultas

STALLINGS, W. Cryptography and Network Security:Principles and Practice. 6. ed.Pearson, 2013 (capítulo 22).

Site oficial Squid: www.squid-cache.org