GERENCIAMENTO DA PORTA 25

uma revisão

Danton Nunes, Internexo Ltda. São José dos Campos, SP
danton.nunes@inexo.com.br

Agenda

Os tortuosos caminhos das mensagens eletrônicas: SMTP, TLS e outras sopas de letrinhas.

A confusão entre submissão e transporte de mensagens.

Agentes clandestinos infiltrados em sua máquina: spambots.

Estratégias de gerenciamento da porta 25 (e 465 também!).

- Bloqueio puro, simples e malvado;
- Desvio para um proxy translúcido;
- Desvio para uma armadilha.

Submissão autenticada de mensagens: cuidado com senhas fracas.

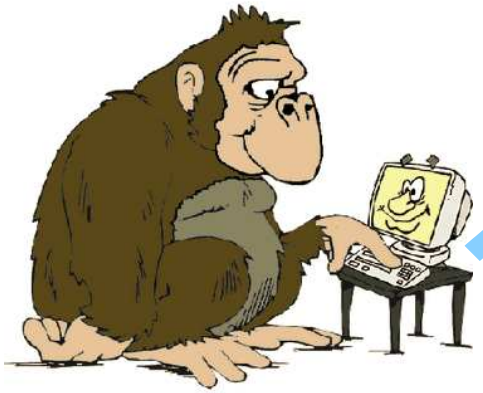
Recomendações finais.

Os tortuosos caminhos das mensagens eletrônicas

Os tortuosos caminhos das mensagens eletrônicas

TUDO COMEÇA COM O USUÁRIO.

Os tortuosos caminhos das mensagens eletrônicas



TUDO COMEÇA COM O USUÁRIO.

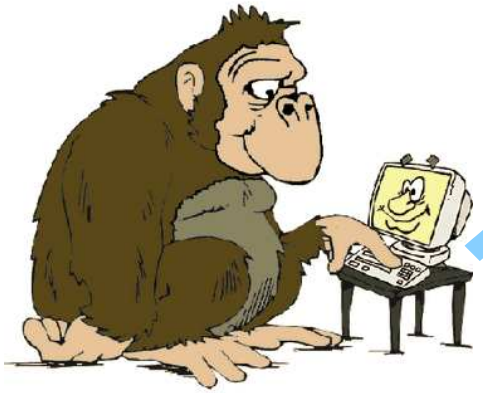
QUE A SUBMETE AO SERVIDOR CORPORATIVO

SMTP COM AUTENTICAÇÃO

587/TCP

Quem assistiu Alphaville de Godard sabe o que é isto!

Os tortuosos caminhos das mensagens eletrônicas



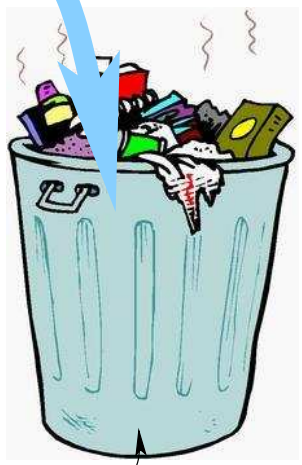
TUDO COMEÇA COM O USUÁRIO.

QUE A SUBMETE AO SERVIDOR CORPORATIVO

SMTP COM AUTENTICAÇÃO

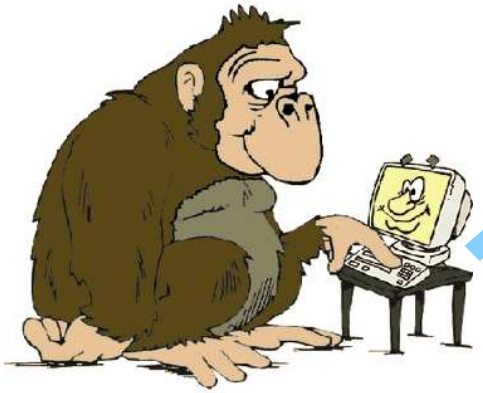
587/TCP

Quem assistiu Alphaville de Godard sabe o que é isto!



O SERVIDOR COLOCA A MENSAGEM EM FILA:

Os tortuosos caminhos das mensagens eletrônicas



TUDO COMEÇA COM O USUÁRIO.

587/TCP

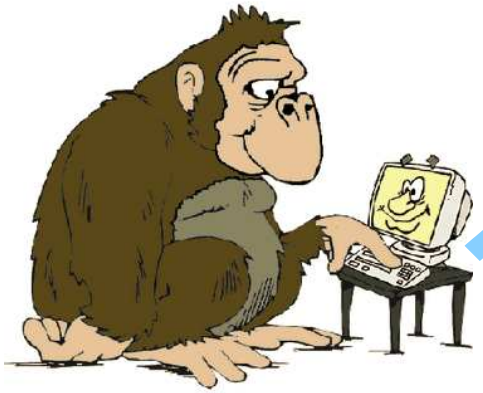
SMTP COM AUTENTICAÇÃO

QUE A SUBMETE AO SERVIDOR CORPORATIVO

Quem assistiu Alphaville de Godard sabe o que é isto!

O SERVIDOR COLOCA A MENSAGEM EM FILA:

Os tortuosos caminhos das mensagens eletrônicas



TUDO COMEÇA COM O USUÁRIO.

587/TCP

SMTP COM AUTENTICAÇÃO

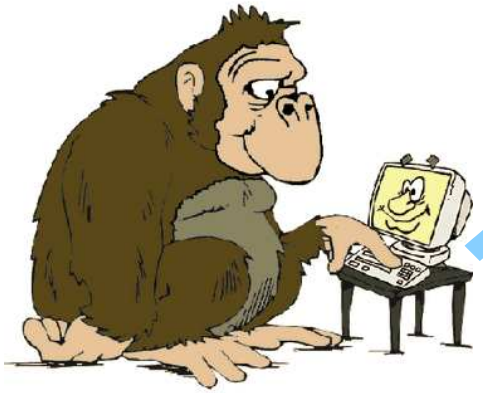
QUE A SUBMETE AO SERVIDOR CORPORATIVO

Quem assistiu Alphaville de Godard sabe o que é isto!

O SERVIDOR COLOCA A MENSAGEM EM FILA:

O AGENTE DE TRANSPORTE DE MENSAGENS TIRA DA FILA E ENVIA PARA O SERVIDOR DE DESTINO (MX, AAAA, A)

Os tortuosos caminhos das mensagens eletrônicas



TUDO COMEÇA COM O USUÁRIO.

587/TCP

SMTP COM AUTENTICAÇÃO

QUE A SUBMETE AO SERVIDOR CORPORATIVO

Quem assistiu Alphaville de Godard sabe o que é isto!

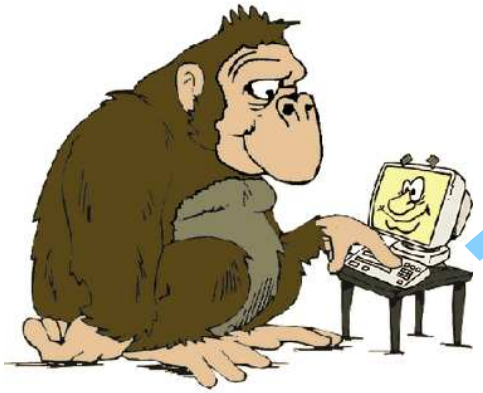
O SERVIDOR COLOCA A MENSAGEM EM FILA:

SMTP SEM AUTENTICAÇÃO

25/TCP

O AGENTE DE TRANSPORTE DE MENSAGENS TIRA DA FILA E ENVIA PARA O SERVIDOR DE DESTINO (MX, AAAA, A)

Os tortuosos caminhos das mensagens eletrônicas



TUDO COMEÇA COM O USUÁRIO.

QUE A SUBMETE AO SERVIDOR CORPORATIVO

SMTP COM AUTENTICAÇÃO

587/TCP

Quem assistiu Alphaville de Godard sabe o que é isto!

O SERVIDOR COLOCA A MENSAGEM EM FILA:

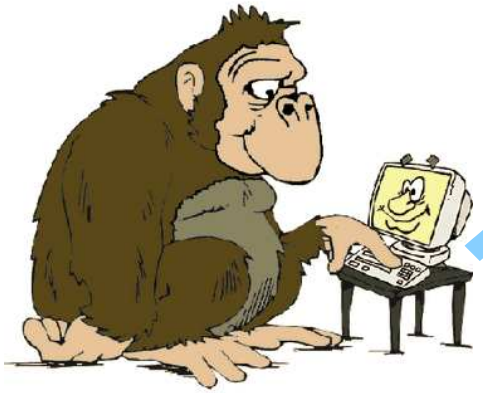
O AGENTE DE TRANSPORTE DE MENSAGENS TIRA DA FILA E ENVIA PARA O SERVIDOR DE DESTINO (MX, AAAA, A)

25/TCP

SMTP SEM AUTENTICAÇÃO

E, FINALMENTE, A MENSAGEM É ENTREGUE AO DESTINATÁRIO (POP, IMAP)

Os tortuosos caminhos das mensagens eletrônicas



TUDO COMEÇA COM O USUÁRIO.

QUE A SUBMETE AO SERVIDOR CORPORATIVO

SMTP COM AUTENTICAÇÃO

587/TCP

Quem assistiu Alphaville de Godard sabe o que é isto!

O SERVIDOR COLOCA A MENSAGEM EM FILA:

AQUI MORA O PERIGO!

E, FINALMENTE, A MENSAGEM É ENTREGUE AO DESTINATÁRIO (POP, IMAP)

SMTP SEM AUTENTICAÇÃO

25/TCP

O AGENTE DE TRANSPORTE DE MENSAGENS TIRA DA FILA E ENVIA PARA O SERVIDOR DE DESTINO (MX, AAAA, A)

Os tortuosos caminhos das mensagens eletrônicas

sopa de letrinhas	portas	para que serve
SMTP	**25**	**Transporte de mensagens entre MTUs.**
SMTPS	**465**	**Transporte de mensagens entre MTUs em texto cifrado.**
SMTP+Auth	**587**	**Submissão de mensagens para envio.**
SSL	**465**	**Camada criptográfica no nível de sessão.** Apesar do SSL prover mecanismo de autenticação por meio de certificados, este não é normalmente usado pelo SMTP. Praticamente em desuso, substituida pelo TLS.
TLS	**25,587**	**Camada criptográfica negociada pela aplicação.** Usa o comando STARTTLS para iniciar o diálogo sigiloso, usado em conjunto com autenticação com senha em texto claro.

A confusão entre submissão e transporte de mensagens

Submissão

A mensagem sai do agente do usuário para o agente de submissão que a coloca em uma fila.

Usa a porta 587/tcp, com autenticação obrigatória e criptografia opcional.

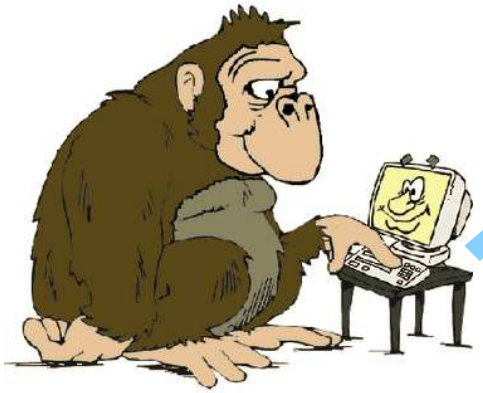
Transporte

A mensagem sai do agente do agente de transporte do remetente e vai para o agente de transporte do destinatário ou outro intermediário, determinado pelos atributos MX, AAAA ou A do domínio do destinatário.

Usa a porta 25/tcp (sem criptografia ou com TLS) ou a 465/tcp (sob SSL).

Não tem autenticação!

Agentes clandestinos infiltrados em sua máquina: spambots



TUDO COMEÇA COM O USUÁRIO.

QUE A SUBMETE AO SERVIDOR CORPORATIVO

SMTP COM AUTENTICAÇÃO

587/TCP

Quem assistiu Alphaville de Godard sabe o que é isto!

O SERVIDOR COLOCA A MENSAGEM EM FILA:

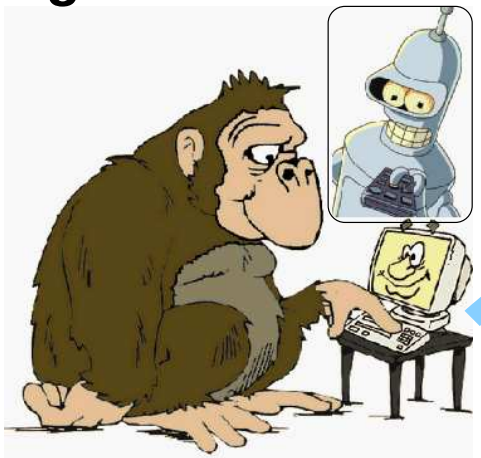
O AGENTE DE TRANSPORTE DE MENSAGENS TIRA DA FILA E ENVIA PARA O SERVIDOR DE DESTINO (MX, AAAA, A)

25/TCP

SMTP SEM AUTENTICAÇÃO

E, FINALMENTE, A MENSAGEM É ENTREGUE AO DESTINATÁRIO (POP, IMAP)

Agentes clandestinos infiltrados em sua máquina: spambots



TUDO COMEÇA COM O USUÁRIO.

QUE A SUBMETE AO SERVIDOR CORPORATIVO

SMTP COM AUTENTICAÇÃO

587/TCP

Quem assistiu Alphaville de Godard sabe o que é isto!

O SERVIDOR COLOCA A MENSAGEM EM FILA:

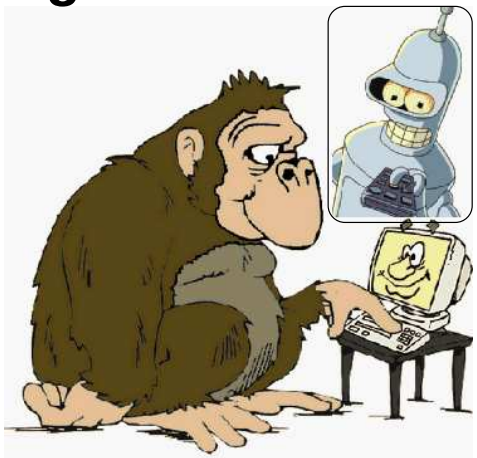
O AGENTE DE TRANSPORTE DE MENSAGENS TIRA DA FILA E ENVIA PARA O SERVIDOR DE DESTINO (MX, AAAA, A)

SMTP SEM AUTENTICAÇÃO

25/TCP

E, FINALMENTE, A MENSAGEM É ENTREGUE AO DESTINATÁRIO (POP, IMAP)

Agentes clandestinos infiltrados em sua máquina: spambots

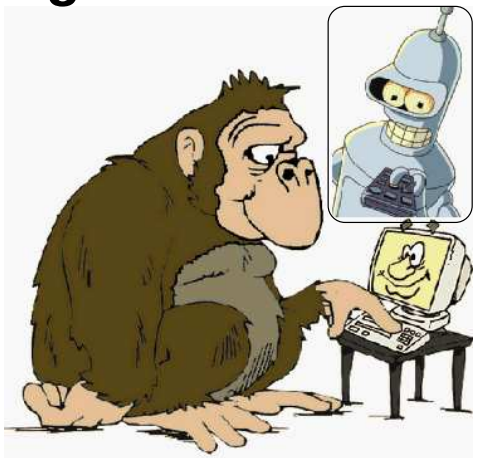


TUDO COMEÇA COM O USUÁRIO.

PORTA 25, SEM AUTENTICAÇÃO!

E, FINALMENTE,
A MENSAGEM
É ENTREGUE
AO DESTINATÁRIO
(POP, IMAP)

Agentes clandestinos infiltrados em sua máquina: spambots



TUDO COMEÇA COM O USUÁRIO.

PORTA 25, SEM AUTENTICAÇÃO!

Lista Negra OK
SPF OK
Greylist OK

E, FINALMENTE,
A MENSAGEM
É ENTREGUE
AO DESTINATÁRIO
(POP, IMAP)

Agentes clandestinos infiltrados em sua máquina: spambots

Consequências

Seus endereços IP vão parar em listas negras => REPUTAÇÃO

Tráfego de saída, roubo de banda

Chuva de reclamações para você, seus proveedores e do cert.br

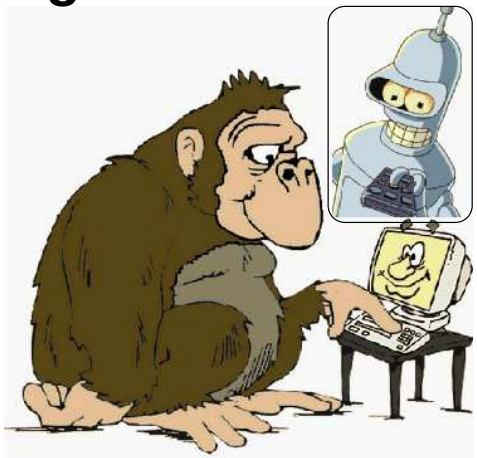
Aborrecimentos.

O que fazer?

Impedir que o spambot consiga se comunicar diretamente com agentes de transporte de mensagens diretamente

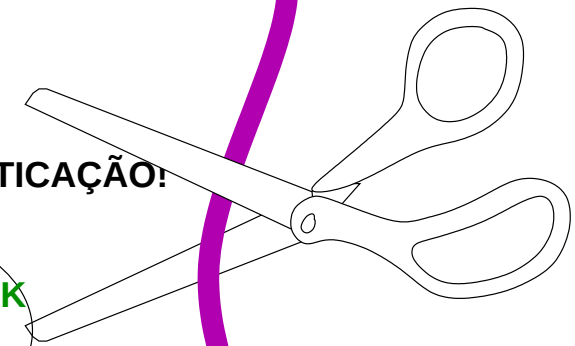
Identificar quais máquinas estão contaminadas com spambots e tirá−las de serviço até que sejam limpas. <= especialmente em rede corporativa.

Agentes clandestinos infiltrados em sua máquina: spambots



TUDO COMEÇA COM O USUÁRIO.

PORTA 25, SEM AUTENTICAÇÃO!



Lista Negra OK
SPF OK
Greylist OK

E, FINALMENTE,
A MENSAGEM
É ENTREGUE
AO DESTINATÁRIO
(POP, IMAP)

Estratégias de gerenciamento da porta 25 (e 465 também!)

- Bloqueio puro, simples e malvado
- Desvio para um proxy translúcido
- Desvio para uma armadilha

Estratégias de gerenciamento da porta 25 (e 465 também!)

- Bloqueio puro, simples e malvado
- Desvio para um proxy translúcido
- Desvio para uma armadilha

Estratégias de gerenciamento da porta 25 (e 465 também!)

- Bloqueio puro, simples e malvado
- Desvio para um proxy translúcido
- Desvio para uma armadilha

Mínima dor de cabeça

Mecanismo de transição

Estratégias de gerenciamento da porta 25 (e 465 também!)

- Bloqueio puro, simples e malvado
- Desvio para um proxy translúcido
- Desvio para uma armadilha

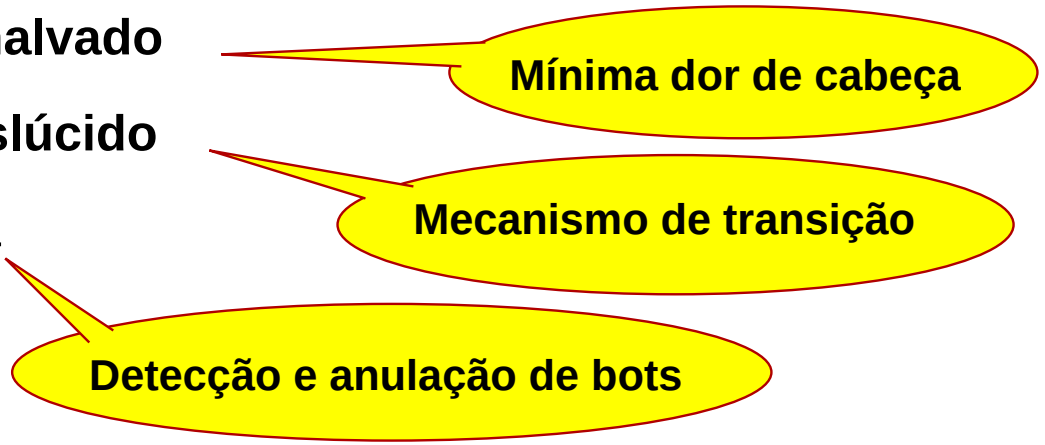
Mínima dor de cabeça

Mecanismo de transição

Detecção e anulação de bots

Estratégias de gerenciamento da porta 25 (e 465 também!)

- Bloqueio puro, simples e malvado
- Desvio para um proxy translúcido
- Desvio para uma armadilha

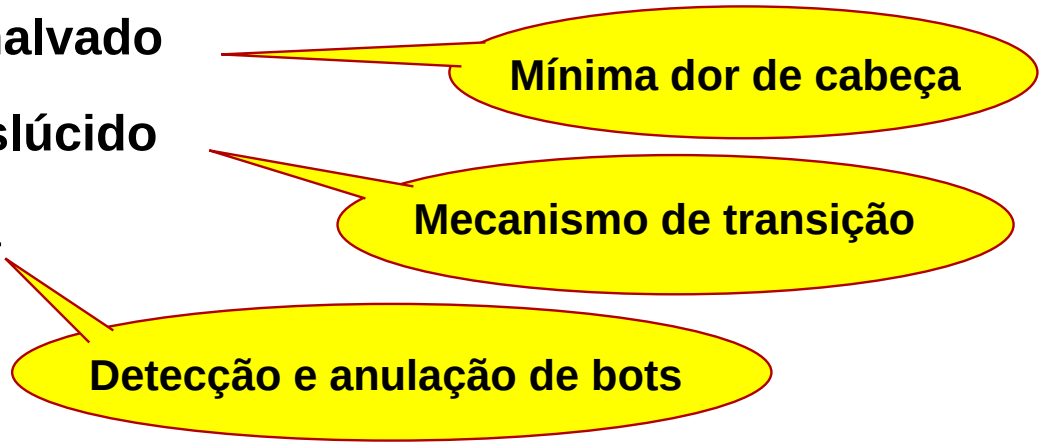


Considerações

Tratar as portas 25 (SMTP em texto claro) e 465 (SMTP sob SSL)

Estratégias de gerenciamento da porta 25 (e 465 também!)

- Bloqueio puro, simples e malvado
- Desvio para um proxy translúcido
- Desvio para uma armadilha



Considerações

Tratar as portas 25 (SMTP em texto claro) e 465 (SMTP sob SSL)

Considerar os casos de IPv4 e IPv6, mesmo que sua rede não tenha IPv6!

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Desvio para um proxy translúcido

Desvio para uma armadilha

Mínima dor de cabeça

Mecanismo de transição

Detecção e anulação de bots

Considerações

Por causa do teredo!

Tratar as portas 25 (SMTP em texto claro) e 465 (SMTP sob SSL)

Considerar os casos de IPv4 e IPv6, mesmo que sua rede não tenha IPv6!

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Desvio para um proxy translúcido

Desvio para uma armadilha

Mínima dor de cabeça

Mecanismo de transição

Detecção e anulação de bots

Considerações

Por causa do teredo!

Tratar as portas 25 (SMTP em texto claro) e 465 (SMTP sob SSL)

Considerar os casos de IPv4 e IPv6, mesmo que sua rede não tenha IPv6!

Usar capacidade de registro do firewall para detectar máquinas contaminadas

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Desvio para um proxy translúcido

Desvio para uma armadilha

Mínima dor de cabeça

Mecanismo de transição

Detecção e anulação de bots

Considerações

Por causa do teredo!

Tratar as portas 25 (SMTP em texto claro) e 465 (SMTP sob SSL)

Considerar os casos de IPv4 e IPv6, mesmo que sua rede não tenha IPv6!

Usar capacidade de registro do firewall para detectar máquinas contaminadas

Manter esquema de atendimento a reclamações (abuse@meu.dominio) e dados de contato corretos no 'whois'

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Desvio para um proxy translúcido

Desvio para uma armadilha

Mínima dor de cabeça

Mecanismo de transição

Detecção e anulação de bots

Considerações

Por causa do teredo!

Tratar as portas 25 (SMTP em texto claro) e 465 (SMTP sob SSL)

Considerar os casos de IPv4 e IPv6, mesmo que sua rede não tenha IPv6!

Usar capacidade de registro do firewall para detectar máquinas contaminadas

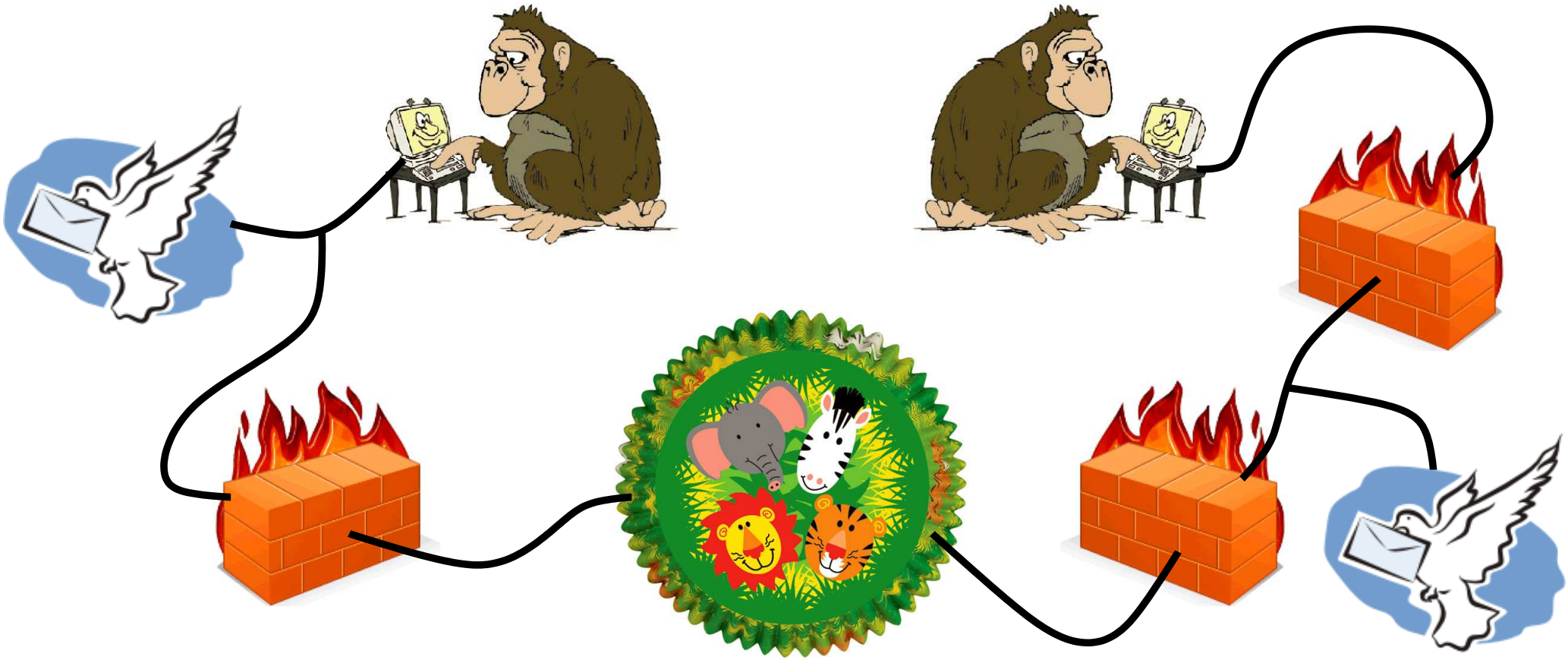
Manter esquema de atendimento a reclamações (abuse@meu.dominio) e dados de contato corretos no 'whois'

E, o mais difícil, EDUCAR O USUÁRIO!

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

screened host ***DMZ (DeMilitarised Zone)***

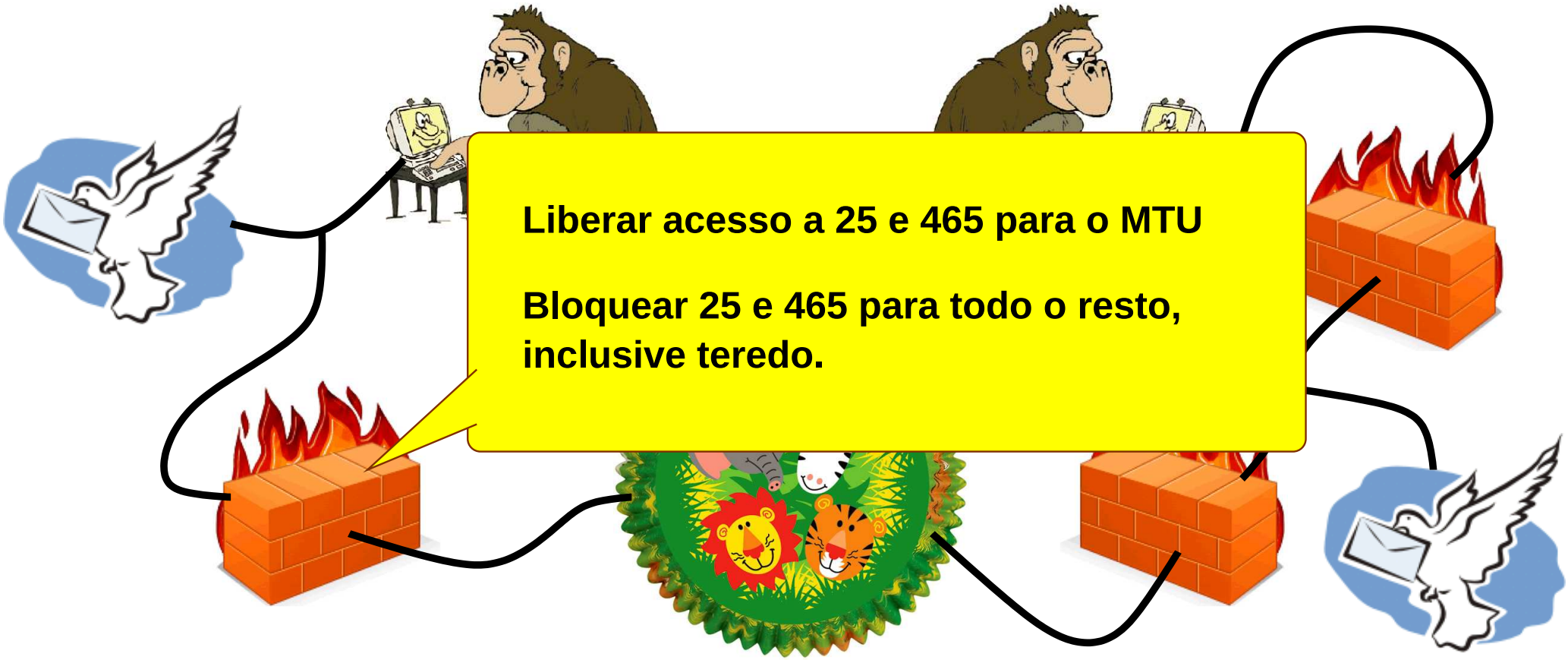


A selva da Internet!

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

screened host ***DMZ (DeMilitarised Zone)***



A selva da Internet!

Estratégias de gerenciamento da porta 25 (e 465 também!)

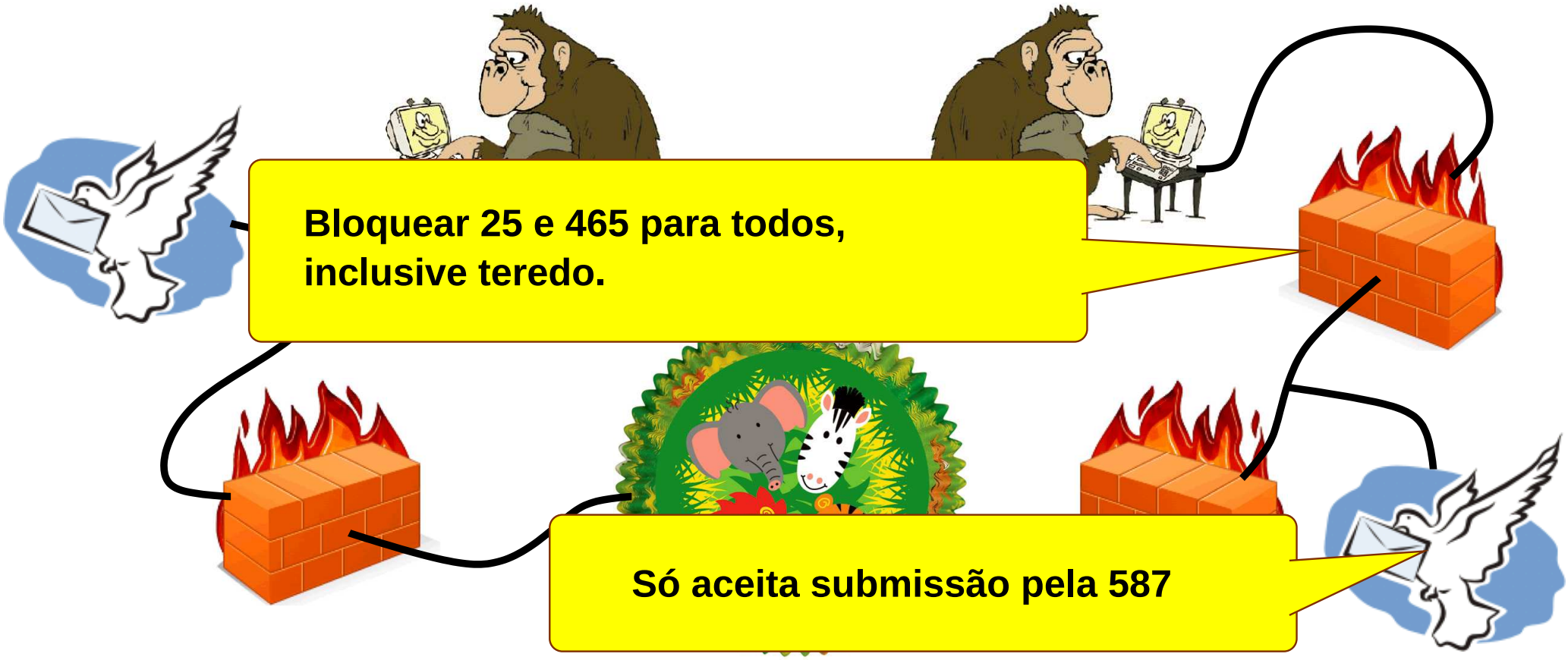
Bloqueio puro, simples e malvado

screened host ***DMZ (DeMilitarised Zone)***

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

screened host ***DMZ (DeMilitarised Zone)***



A selva da Internet!

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

```
# libera o acesso ao servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT
```

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

```
# libera o acesso ao servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP
```

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

```
# libera o acesso ao servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP

# bloqueia acesso para clientes tunelados via teredo
# AVISO: isto aqui é bruxaria da mais alta. Em outros tempos por menos que isto se ia para a fogueira.
/sbin/iptables -A FORWARD -i eth0 -p udp -s 203.0.113.0/24 -dport 3544 -m u32 \
   --u32 "4 & 0x3FFF = 0 && 0 >> 22 & 0x3C @ 8 >> 26 = 6 &&  11 & 0xFF = 6 && 48 & 0xFFFF = 25,465" \
   -j DROP
```

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

```
# libera o acesso ao servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP

# bloqueia acesso para clientes tunelados via teredo
# AVISO: isto aqui é bruxaria da mais alta. Em outros tempos por menos que isto se ia para a fogueira.
/sbin/iptables -A FORWARD -i eth0 -p udp -s 203.0.113.0/24 -dport 3544 -m u32 \
   --u32 "4 & 0x3FFF = 0 && 0 >> 22 & 0x3C @ 8 >> 26 = 6 &&  11 & 0xFF = 6 && 48 & 0xFFFF = 25,465" \
   -j DROP
```

teredo

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

```
# libera o acesso ao servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP

# bloqueia acesso para clientes tunelados via teredo
# AVISO: isto aqui é bruxaria da mais alta. Em outros tempos por menos que isto se ia para a fogueira.
/sbin/iptables -A FORWARD -i eth0 -p udp -s 203.0.113.0/24 -dport 3544 -m u32 \
   --u32 "4 & 0x3FFF = 0 && 0 >> 22 & 0x3C @ 8 >> 26 = 6 &&  11 & 0xFF = 6 && 48 & 0xFFFF = 25,465" \
   -j DROP
```

Não é fragmento

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

```
# libera o acesso ao servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP

# bloqueia acesso para clientes tunelados via teredo
# AVISO: isto aqui é bruxaria da mais alta. Em outros tempos por menos que isto se ia para a fogueira.
/sbin/iptables -A FORWARD -i eth0 -p udp -s 203.0.113.0/24 -dport 3544 -m u32 \
   --u32 "4 & 0x3FFF = 0 && 0 >> 22 & 0x3C @ 8 >> 26 = 6 &&  11 & 0xFF = 6 && 48 & 0xFFFF = 25,465" \
   -j DROP
```

Aponta para o começo do datagrama (UDP)

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

```
# libera o acesso ao servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP

# bloqueia acesso para clientes tunelados via teredo
# AVISO: isto aqui é bruxaria da mais alta. Em outros tempos por menos que isto se ia para a fogueira.
/sbin/iptables -A FORWARD -i eth0 -p udp -s 203.0.113.0/24 -dport 3544 -m u32 \
   --u32 "4 & 0x3FFF = 0 && 0 >> 22 & 0x3C @ 8 >> 26 = 6 &&  11 & 0xFF = 6 && 48 & 0xFFFF = 25,465" \
   -j DROP
```

payload é IPv6

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

```
# libera o acesso ao servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP

# bloqueia acesso para clientes tunelados via teredo
# AVISO: isto aqui é bruxaria da mais alta. Em outros tempos por menos que isto se ia para a fogueira.
/sbin/iptables -A FORWARD -i eth0 -p udp -s 203.0.113.0/24 -dport 3544 -m u32 \
   --u32 "4 & 0x3FFF = 0 && 0 >> 22 & 0x3C @ 8 >> 26 = 6 &&  11 & 0xFF = 6 && 48 & 0xFFFF = 25,465" \
   -j DROP
```

TCP sobre IPv6

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

```
# libera o acesso ao servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP

# bloqueia acesso para clientes tunelados via teredo
# AVISO: isto aqui é bruxaria da mais alta. Em outros tempos por menos que isto se ia para a fogueira.
/sbin/iptables -A FORWARD -i eth0 -p udp -s 203.0.113.0/24 -dport 3544 -m u32 \
   --u32 "4 & 0x3FFF = 0 && 0 >> 22 & 0x3C @ 8 >> 26 = 6 &&  11 & 0xFF = 6 && 48 & 0xFFFF = 25,465" \
   -j DROP
```

portas 25 ou 465

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − screened host

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Servidor de email IPv4:203.0.113.25 e IPv6:2001:db8:b01a:70da::25

```
# libera o acesso ao servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP

# bloqueia acesso para clientes tunelados via teredo
# AVISO: isto aqui é bruxaria da mais alta. Em outros tempos por menos que isto se ia para a fogueira.
/sbin/iptables -A FORWARD -i eth0 -p udp -s 203.0.113.0/24 -dport 3544 -m u32 \
   --u32 "4 & 0x3FFF = 0 && 0 >> 22 & 0x3C @ 8 >> 26 = 6 &&  11 & 0xFF = 6 && 48 & 0xFFFF = 25,465" \
   -j DROP
```

é fácil!

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − DMZ

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Toda a configuração é feita no roteador INTERNO!

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − DMZ

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Toda a configuração é feita no roteador INTERNO!

```
# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP
```

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − DMZ

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Toda a configuração é feita no roteador INTERNO!

```
# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP

# bloqueia acesso para clientes tunelados via teredo
# AVISO: isto aqui é bruxaria da mais alta. Em outros tempos por menos que isto se ia para a fogueira.
/sbin/iptables -A FORWARD -i eth0 -p udp -s 203.0.113.0/24 -dport 3544 -m u32 \
   --u32 "4 & 0x3FFF = 0 && 0 >> 22 & 0x3C @ 8 >> 26 = 6 &&  11 & 0xFF = 6 && 48 & 0xFFFF = 25,465" \
   -j DROP
```

Estratégias de gerenciamento da porta 25 (e 465 também!)

Bloqueio puro, simples e malvado

Como fazer − exemplo com Linux com iptables − DMZ

Rede interna eth0 IPv4:203.0.113.0/24 e IPv6:2001:db8:b01a:70da/64

Toda a configuração é feita no roteador INTERNO!

```
# bloqueia o acesso para os demais clientes.
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j LOG
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.0/24 --dports 25,465 -j DROP
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j LOG
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::/64 --dports 25,465 -j DROP

# bloqueia acesso para clientes tunelados via teredo
# AVISO: isto aqui é bruxaria da mais alta. Em outros tempos por menos que isto se ia para a fogueira.
/sbin/iptables -A FORWARD -i eth0 -p udp -s 203.0.113.0/24 -dport 3544 -m u32 \
   --u32 "4 & 0x3FFF = 0 && 0 >> 22 & 0x3C @ 8 >> 26 = 6 &&  11 & 0xFF = 6 && 48 & 0xFFFF = 25,465" \
   -j DROP
```

O servidor de correio atende a submissões tanto da rede interna quanto de fora (para usuários em trânsito) pela porta 587/tcp que não fica bloqueada.

Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para um proxy translúcido

Situação: decidimos mudar a política, submissão agora só pela porta 587, mas não queremos que os usuários que ainda não reconfiguraram seus programas deixem de enviar mensagens.

Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para um proxy translúcido

Situação: decidimos mudar a política, submissão agora só pela porta 587, mas não queremos que os usuários que ainda não reconfiguraram seus programas deixem de enviar mensagens.

Truque: tudo que for para a porta 25 é desviado para a porta 587 do servidor de submissão, onde só passa quem "mostrar o crachá".

Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para um proxy translúcido

Situação: decidimos mudar a política, submissão agora só pela porta 587, mas não queremos que os usuários que ainda não reconfiguraram seus programas deixem de enviar mensagens.

Truque: tudo que for para a porta 25 é desviado para a porta 587 do servidor de submissão, onde só passa quem "mostrar o crachá".

```
# abre as portas 25,465 para o servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT
```

Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para um proxy translúcido

Situação: decidimos mudar a política, submissão agora só pela porta 587, mas não queremos que os usuários que ainda não reconfiguraram seus programas deixem de enviar mensagens.

Truque: tudo que for para a porta 25 é desviado para a porta 587 do servidor de submissão, onde só passa quem "mostrar o crachá".

```
# abre as portas 25,465 para o servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# agora a pequena maldade, desviamos o que vier pela 25 para a 587
/sbin/iptables -t nat -A PREROUTING -i eth0 -p tcp -s 203.0.113.0/24 --dport 25 \
        -j DNAT --to-destination 203.0.113.25:587
```

Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para um proxy translúcido

Situação: decidimos mudar a política, submissão agora só pela porta 587, mas não queremos que os usuários que ainda não reconfiguraram seus programas deixem de enviar mensagens.

Truque: tudo que for para a porta 25 é desviado para a porta 587 do servidor de submissão, onde só passa quem "mostrar o crachá".

```
# abre as portas 25,465 para o servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# agora a pequena maldade, desviamos o que vier pela 25 para a 587
/sbin/iptables -t nat -A PREROUTING -i eth0 -p tcp -s 203.0.113.0/24 --dport 25 \
        -j DNAT --to-destination 203.0.113.25:587
```

E em IPv6? O time do netfilter desenvolveu patches para que o ip6tables possa fazer as mesmas manobras de seu irmão para IPv4, seguindo a RFC-6296.

Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para um proxy translúcido

Situação: decidimos mudar a política, submissão agora só pela porta 587, mas não queremos que os usuários que ainda não reconfiguraram seus programas deixem de enviar mensagens.

Truque: tudo que for para a porta 25 é desviado para a porta 587 do servidor de submissão, onde só passa quem "mostrar o crachá".

```
# abre as portas 25,465 para o servidor (screened host)
/sbin/iptables -A FORWARD -i eth0 -p tcp -m multiport -s 203.0.113.25 --dports 25,465 -j ACCEPT
/sbin/ip6tables -A FORWARD -i eth0 -p tcp -m multiport -s 2001:db8:b01a:70da::25 --dports 25,465 -j ACCEPT

# agora a pequena maldade, desviamos o que vier pela 25 para a 587
/sbin/iptables -t nat -A PREROUTING -i eth0 -p tcp -s 203.0.113.0/24 --dport 25 \
        -j DNAT --to-destination 203.0.113.25:587
```

E em IPv6? O time do netfilter desenvolveu patches para que o ip6tables possa fazer as mesmas manobras de seu irmão para IPv4, seguindo a RFC-6296.

A porta 465 não é desviada neste caso, a não ser que o servidor de submissão entenda SSL

Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para uma armadilha

Idéia: que tal em vez de a administração da rede sair procurando a máquina com spambot ativo, fazer seu usuário perceber que há algo errado?

Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para uma armadilha

Idéia: que tal em vez de a administração da rede sair procurando a máquina com spambot ativo, fazer seu usuário perceber que há algo errado?

Por exemplo... **CHUTANDO−O PARA FORA DA INTERNET!**

Um artefato que permite fazer isso é o fail2ban.

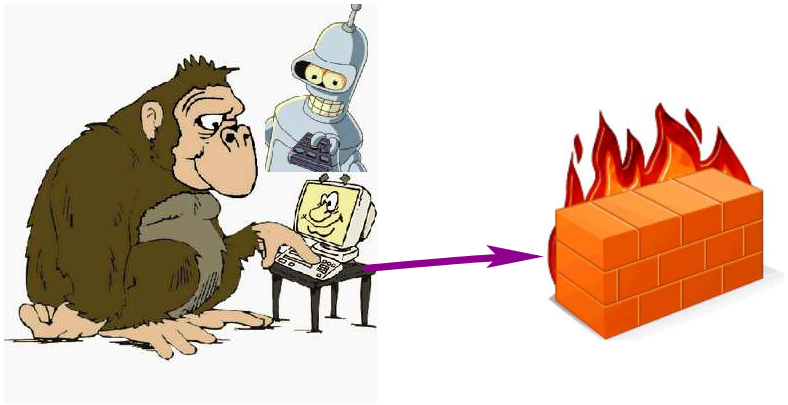
Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para uma armadilha

Idéia: que tal em vez de a administração da rede sair procurando a máquina com spambot ativo, fazer seu usuário perceber que há algo errado?

Por exemplo... **CHUTANDO–O PARA FORA DA INTERNET!**

Um artefato que permite fazer isso é o fail2ban.



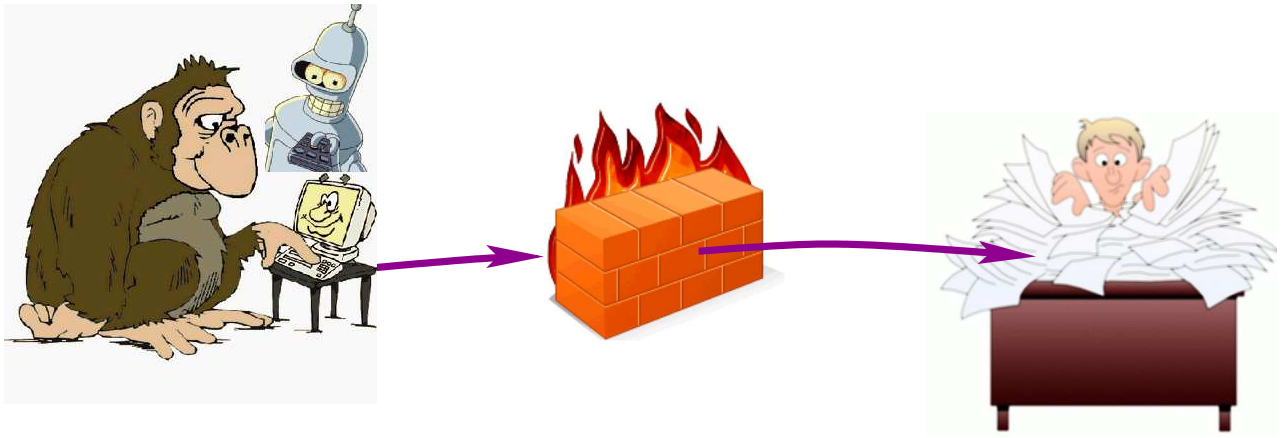
Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para uma armadilha

Idéia: que tal em vez de a administração da rede sair procurando a máquina com spambot ativo, fazer seu usuário perceber que há algo errado?

Por exemplo... **CHUTANDO-O PARA FORA DA INTERNET!**

Um artefato que permite fazer isso é o fail2ban.



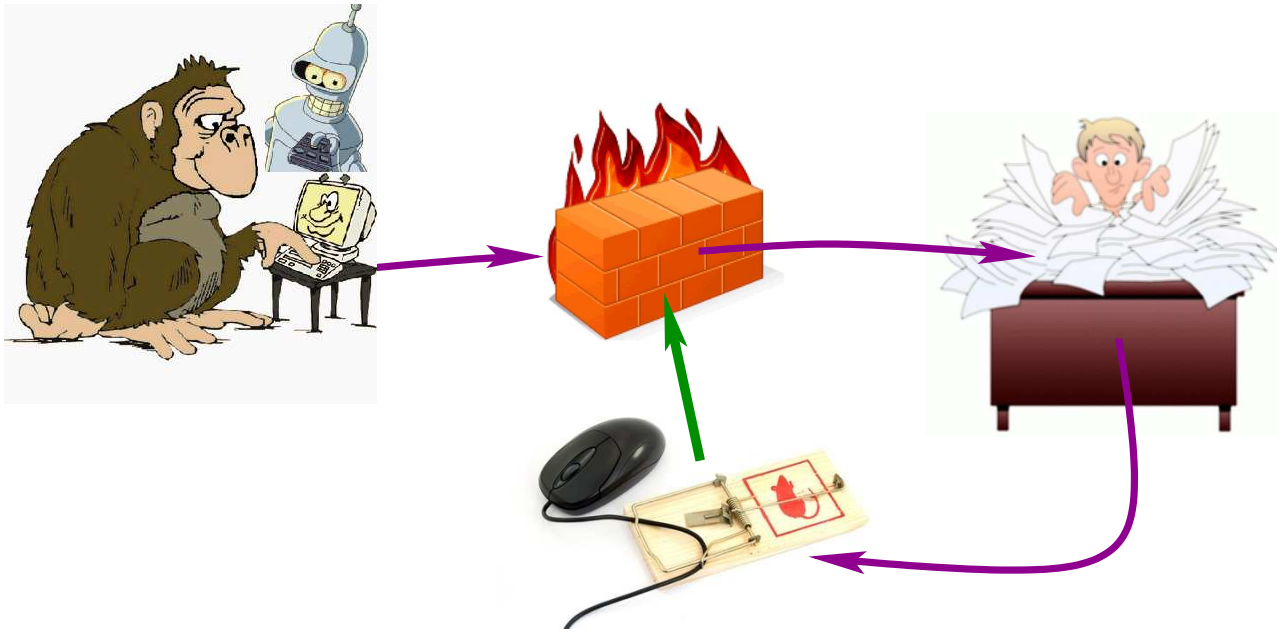
Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para uma armadilha

Idéia: que tal em vez de a administração da rede sair procurando a máquina com spambot ativo, fazer seu usuário perceber que há algo errado?

Por exemplo... **CHUTANDO-O PARA FORA DA INTERNET!**

Um artefato que permite fazer isso é o fail2ban.



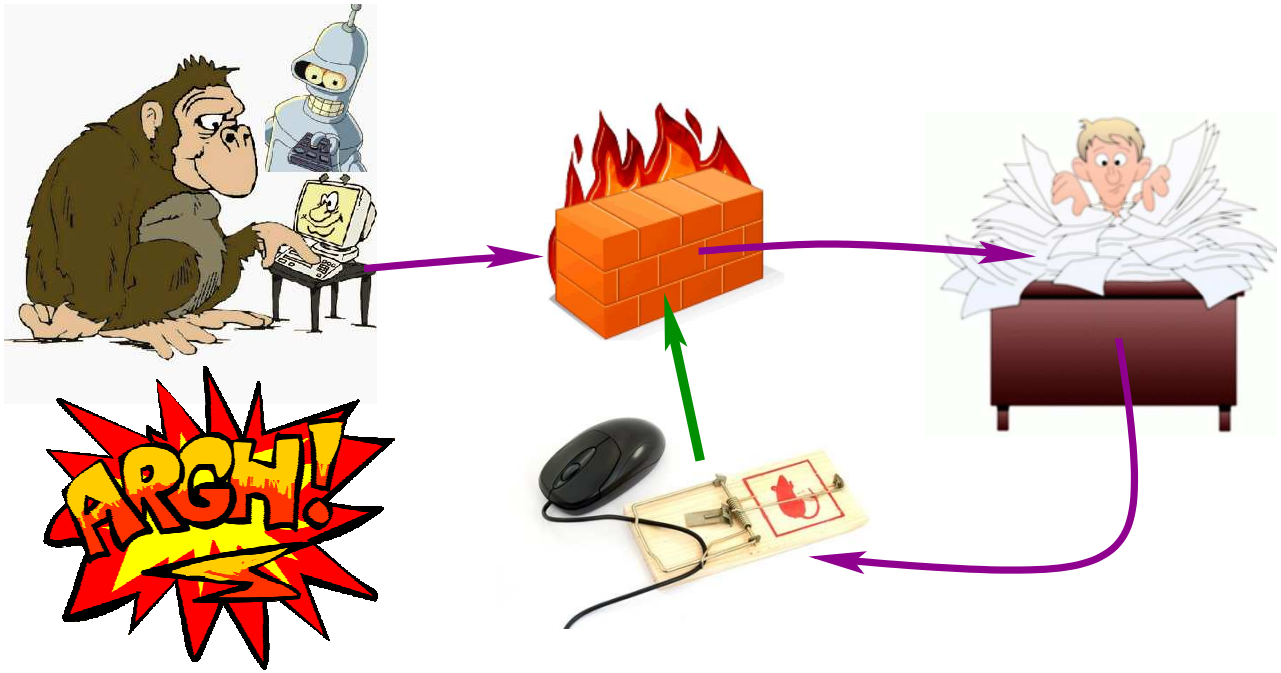
Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para uma armadilha

Idéia: que tal em vez de a administração da rede sair procurando a máquina com spambot ativo, fazer seu usuário perceber que há algo errado?

Por exemplo... **CHUTANDO-O PARA FORA DA INTERNET!**

Um artefato que permite fazer isso é o fail2ban.



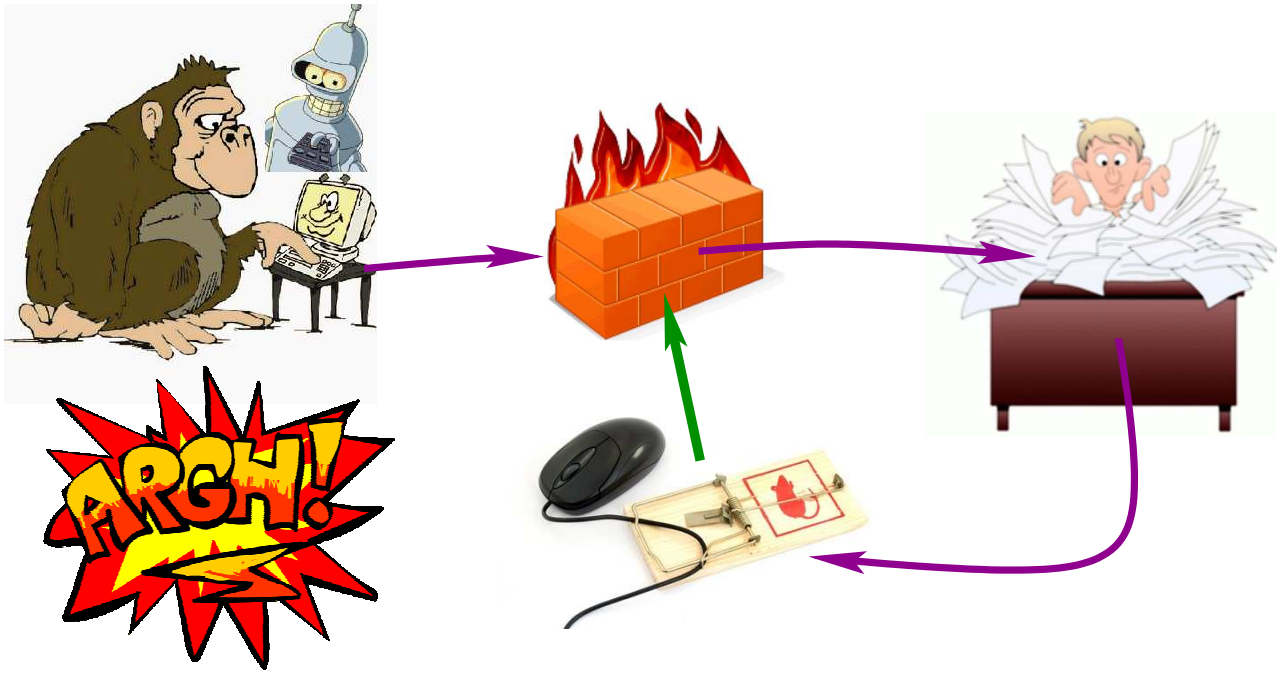
Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para uma armadilha

Idéia: que tal em vez de a administração da rede sair procurando a máquina com spambot ativo, fazer seu usuário perceber que há algo errado?

Por exemplo... **CHUTANDO–O PARA FORA DA INTERNET!**

Um artefato que permite fazer isso é o fail2ban.



Pró:

» O ônus de localizar PCs bichados passa para o usuário.

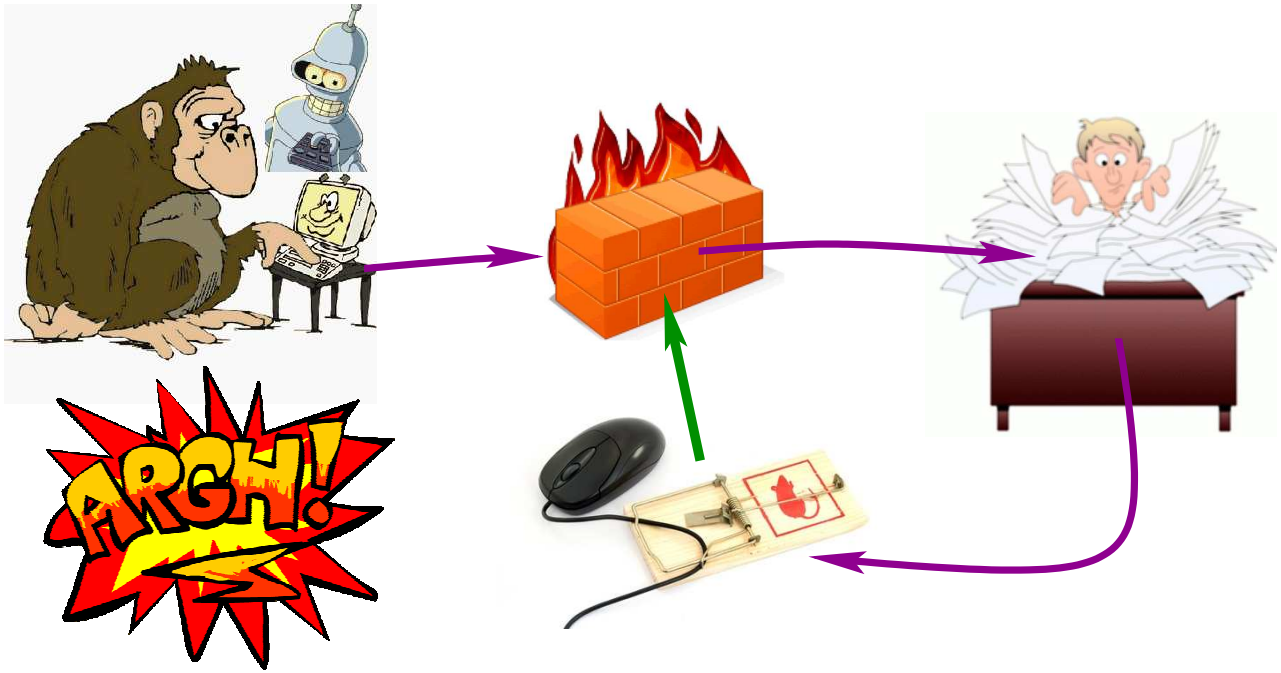
Estratégias de gerenciamento da porta 25 (e 465 também!)

Desvio para uma armadilha

Idéia: que tal em vez de a administração da rede sair procurando a máquina com spambot ativo, fazer seu usuário perceber que há algo errado?

Por exemplo... **CHUTANDO-O PARA FORA DA INTERNET!**

Um artefato que permite fazer isso é o fail2ban.



Pró:
- **» O ônus de localizar PCs bichados passa para o usuário.**

Contras:
- **» Alarmes falsos.**
- **» Desconectar um PC em algum momento crítico.**

Submissão autenticada de mensagens

Cuidado com as senhas fracas!

Submissão autenticada de mensagens

Cuidado com as senhas fracas!

Uma das consequências do sucesso de políticas de gerenciamento da porta 25 é que alguns spambots estão "aprendendo" a usar a 587.

Submissão autenticada de mensagens

Cuidado com as senhas fracas!

Uma das consequências do sucesso de políticas de gerenciamento da porta 25 é que alguns spambots estão "aprendendo" a usar a 587.

A atividade de tentativa de quebra de senhas através de probes contra SMTP, POP e IMAP vem aumentando muito ultimamente.

Submissão autenticada de mensagens

Cuidado com as senhas fracas!

Uma das consequências do sucesso de políticas de gerenciamento da porta 25 é que alguns spambots estão "aprendendo" a usar a 587.

A atividade de tentativa de quebra de senhas através de probes contra SMTP, POP e IMAP vem aumentando muito ultimamente.

Se torna necessário gerenciar as senhas de submissão de mensagens, evitando senhas triviais, especialmente em redes que usam "single point of sign on" (p.ex. LDAP).

Submissão autenticada de mensagens

Cuidado com as senhas fracas!

Uma das consequências do sucesso de políticas de gerenciamento da porta 25 é que alguns spambots estão "aprendendo" a usar a 587.

A atividade de tentativa de quebra de senhas através de probes contra SMTP, POP e IMAP vem aumentando muito ultimamente.

Se torna necessário gerenciar as senhas de submissão de mensagens, evitando senhas triviais, especialmente em redes que usam "single point of sign on" (p.ex. LDAP).

O fail2ban também pode ser usado para nocautear os pescadores de senhas. Pode ser configurado para cortar o acesso de qualquer IP que tenha fracassado na autenticação por umas poucas vezes.

Recomendações

Gerenciamento do acesso a 25/tcp externa é uma necessidade, dada a proliferação de bots com capacidade de envio direto de email.

Recomendações

Gerenciamento do acesso a 25/tcp externa é uma necessidade, dada a proliferação de bots com capacidade de envio direto de email.

Além do bloqueio puro e simples, há outras estratégias visando identificar e mesmo isolar a máquina hospedeira do spambot.

Recomendações

Gerenciamento do acesso a 25/tcp externa é uma necessidade, dada a proliferação de bots com capacidade de envio direto de email.

Além do bloqueio puro e simples, há outras estratégias visando identificar e mesmo isolar a máquina hospedeira do spambot.

É necessário levar em conta IPv4 e IPv6, especialmente túneis teredo.

Recomendações

Gerenciamento do acesso a 25/tcp externa é uma necessidade, dada a proliferação de bots com capacidade de envio direto de email.

Além do bloqueio puro e simples, há outras estratégias visando identificar e mesmo isolar a máquina hospedeira do spambot.

É necessário levar em conta IPv4 e IPv6, especialmente túneis teredo.

É necessário também manter vivo o endereço abuse@... e dados de contato atualizados no whois. É por aí que você será avisado caso algum bloqueio seja furado.

Recomendações

Gerenciamento do acesso a 25/tcp externa é uma necessidade, dada a proliferação de bots com capacidade de envio direto de email.

Além do bloqueio puro e simples, há outras estratégias visando identificar e mesmo isolar a máquina hospedeira do spambot.

É necessário levar em conta IPv4 e IPv6, especialmente túneis teredo.

É necessário também manter vivo o endereço abuse@... e dados de contato atualizados no whois. É por aí que você será avisado caso algum bloqueio seja furado.

Os bots estão se adaptando aos novos tempos. Muito cuidado com senhas fracas de submissão e com os pescadores automáticos de credenciais.