



Boas práticas para ser um ASN saudável e performático.

Palestrante: LACIER DIAS

mum

Mikrotik User Meeting in Brazil
November 11 - 12, 2013

Curitiba-PR

NTP - Network Time Protocol
Protocolo de Tempo para Redes

- Apoio processo de detecção de falhas de segurança e de isolamento adequado, permitindo a identificação e preservação de evidências que possam vir a ser pertinentes em investigações de crimes de informática.
- Dar registro de eventos (logs) pertinentes de forma a manter informações importantes sobre o fato ocorrido em que se deu um evento.
retailmail.br

SpamHaus - BGPf

Spamhaus oferece uma sessão BGPf de três dias suas listas. Lista Botnet C&C, DROP e DROP estendida (EDROP). Estas listas são usadas para bloquear os pacotes provenientes de IPs envolvidos em certos tipos de atividade maliciosa.

Spamhaus BGPf feed (BGPf)

Spamhaus BGPf feed (BGPf)

http://www.spamhaus.org/bgpf/

Obrigado!!!

Lacier Dias
lacier@lacier.com.br
@lacierdias

lacnic

ARIN

RIPE

APNIC

AFRINIC

RAIWIN, DE BOLA
Mikrotik

TITANIA

CONCLUSÃO...

Um AC (Spamhaus) é muito mais que uma lista de IPs. É uma ferramenta para ajudar a manter a rede segura e livre de ataques. É importante manter a lista atualizada e usar a lista para bloquear os pacotes provenientes de IPs envolvidos em certos tipos de atividade maliciosa.

Como a Internet surgiu?

Como o usuário emerge!!!

Como ela realmente é!

O que é um ASN?

Um Sistema Autônomo (SA) é uma coleção de computadores e roteadores conectados por links de rede. O SA é responsável por rotear o tráfego de dados entre os computadores e roteadores dentro do SA e para e de outros SAs.

Tornar-se um AS?

Quanto custa?

Custo

DESAFIOS

CONTROLE

ESTRUTURA

Boas práticas mais comuns que vale a pena recordar!

Boas práticas mais comuns que vale a pena recordar!

Boas práticas para ser um ASN saudável e performático.

Palestrante: LACIER DIAS

mum

MikroTik User Meeting in Brazil
November 11 - 12, 2013

Curitiba-PR



CONCLUSÃO....

Um AS Saudável é muito mais que seu

TITANIA

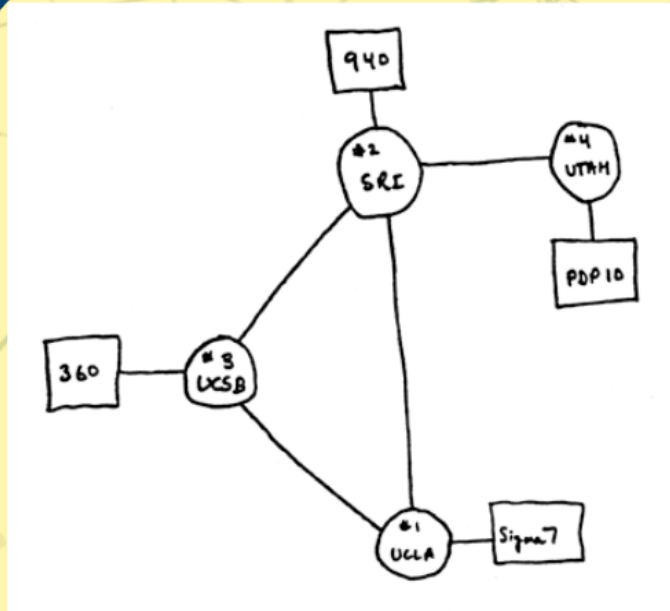
Quem é Lacier Dias ????

- Formado em Segurança da Informação
- Pós-Graduado em Segurança de Rede de Computadores
- MBA em Gerenciamento de Projetos – FGV

- Treinamentos e Certificações:
- IPV6 - Registro.br e SAGE - Hurricane Electric
- Mikrotik Consultant, MTCNA, MTCWE, MTCUME, MTCRE e MTCINE,
- UCT - Ubiquiti Certified Trainer,
- ITIL, Cobit e BSC (Balanced Scorecard),
- ISO 27001 e 27002,
- Motorola, Proxim e Alvarion,
- Allied Telesis, Cisco e Juniper,
- Hughes Networks.

Como a Internet Surgiu?

1969 - ARPANET



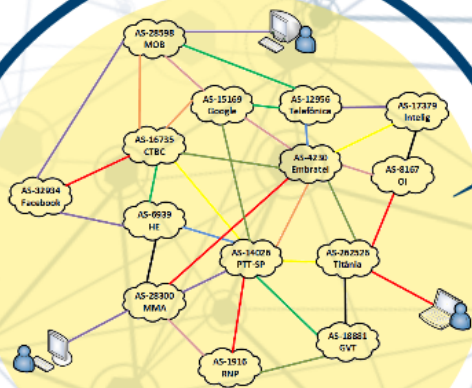
Projeto financiado pela DARPA, que buscava por uma rede resiliente, que pudesse conectar universidades, bases militares e ser resistente à destruição de alguns de seus componentes.

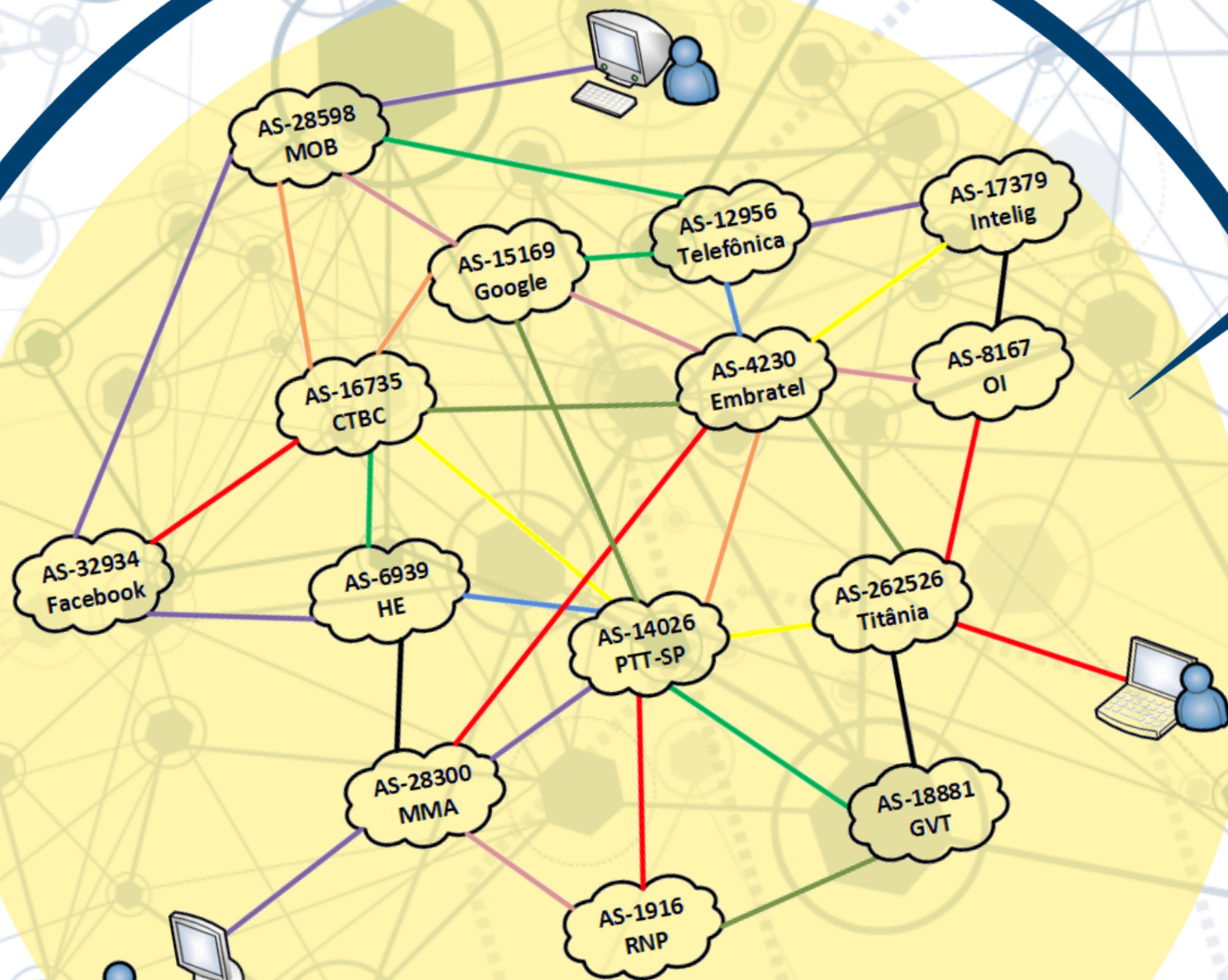


Como o usuário enxerga!!!

Como ela realmente é!

Internet





O que é um ASN?

Um Sistema Autônomo (AS) é uma coleção de prefixos de roteamento conectados por Protocolo Internet (IP) sob o controle de um ou mais operadores de rede que apresenta uma política comum e claramente definida de roteamento para a Internet (RFC 1930, Seção 3).

Tornar-se um AS?

Porque??

**Redundância de acesso à Internet,
Utilização de endereços IP próprios,
Troca de tráfego em PTTs,
Maior controle sobre sua rede,
Mais qualidade para seus clientes/usuários.**

Quando???

**A Internet é fundamental para seu negócio?
Sua rede está tornando-se razoavelmente complexa?
Já tem um grande número de clientes?
Por exemplo, você é um provedor de acesso e tem
cerca de 250 clientes, planejando crescer para 500 em
cerca de 1 ano???**

**Sua equipe possui conhecimentos sólidos sobre
gerenciamento de redes e BGP?
Você possui equipamentos adequados?
Roteadores de borda que suportam BGP.**

<http://registro.br/provedor/numeracao/regras.html>

Custo

Categoria	Tamanho/Prefixos	Custo Inicial	Renovação
Small/Micro	IPv4: menor que /20 IPv6: menor igual /32	1.850,00	1.850,00
Small	IPv4: de /20 até /19 IPv6: maior igual /32 até /31	3.885,00	3.885,00
Medium	IPv4: maior que /19 e menor que /16 IPv6: maior que /31 até /29	10.545,00	10.545,00
Large	IPv4: maior igual a /16 e menor que /14 IPv6: maior que /29 até /27	25.900,00	25.900,00
Extra Large	IPv4: maior igual a /14 e menor que /11 IPv6: maior que /27 até /25	51.800,00	51.800,00
Mayor	IPv4: maior igual a /11 IPv6: maior que /25	74.000,00	74.000,00

Fonte: <http://registro.br/provedor/numeracao/custos.html>

The background is a light blue network diagram with various nodes (circles and hexagons) connected by lines. A large yellow circle with a dark blue border is centered on the slide. A yellow rectangle is positioned at the bottom left, partially overlapping the circle. The text is arranged within these shapes.

**Tirar o AS junto
ao Registro.BR.**

**Fechar a sessão BGP com
as operadoras de trânsito.**

**Manter a saúde
do seu AS.**

DESAFIOS

ESTRUTURA

CONTROLE

RFC 287
Filtros
Loopback
Autenticação
Boas Práticas
DNS Reverso
NTP
IRR
Porta 25

Boas práticas mais comuns que vale a pena recordar!

Loopback

São interfaces lógicas que nunca caem, pois são independente de link

DNS Reverso

O DNS Reverso resolve o endereço IP, buscando o nome associado ao host, verificando se o endereço IP atual corresponde ao endereço IP informado pelo servidor DNS.

Autenticação

É recomendável usar autenticação MD5 para as sessões BGP.

Além das recomendações tradicionais temos ainda precauções extras.

- Não anunciar nem receber rotas com prefixos maiores que /24;
- Filtrar anúncios de rotas inválidas (RFC1918);
- Não redistribuir rotas do IGP no BGP e vice-versa;
- Não aceitar tráfego externo com endereçamento de origem do seu próprio AS;
- Nunca enviar tráfego a destinos não anunciados pelo vizinho BGP através do peering com o mesmo;

Filtro de Cliente

Deve-se aceitar apenas os prefixos que foram designados por você ao cliente, pelo NIC.br ou por um RIR.

Peers

Nas interfaces com sessões eBGP é importante que todos os serviços e protocolos desnecessários estejam desabilitados: IGP (OSPF), RA IPv6, MNDP, CDP, BPDUs, Proxy ARP.....

Fornecedores de Trânsito

Solicite sempre full route e filtre os recebimentos de prefixos de seu upstream, de acordo com sua engenharia de tráfego.

Boas práticas mais

Loopback

São interfaces lógicas que nunca caem, pois são independente de link

O D
IP, k
hos
atu
info

Além das recomen

- Não anunciar nem rec
- Filtrar anúncios de rot

s mais comuns que vale a

DNS Reverso

O DNS Reverso resolve o endereço IP, buscando o nome associado ao host, verificando se o endereço IP atual corresponde ao endereço IP informado pelo servidor DNS.

s recomendações tradicionais temos ainda

e a pena recordar!

Autenticação

É recomendável usar autenticação MD5 para as sessões BGP.



Loopback

As interfaces lógicas nunca caem, pois são independentes de link.

DNS Reverso

O DNS Reverso resolve o endereço IP, buscando o nome associado ao host, verificando se o endereço IP atual corresponde ao endereço IP informado pelo servidor DNS.

Autenticação

É recomendável usar autenticação MD5 para as sessões BGP.

Além das recomendações tradicionais temos ainda precauções extras.

- Não anunciar nem receber rotas com prefixos maiores que /24;
- Filtrar anúncios de rotas inválidas (RFC1918);
- Não redistribuir rotas do IGP no BGP e vice-versa;
- Não aceitar tráfego externo com endereçamento de origem do seu próprio AS;
- Nunca enviar tráfego a destinos não anunciados pelo vizinho BGP através do peering com o mesmo;

Filtro de Cliente

Não deve-se aceitar apenas os prefixos que foram anunciados por você, mas também os prefixos de seus clientes, pelo NIC.br ou por um RIR.

Peers

Nas interfaces com sessões eBGP é importante que todos os serviços e protocolos desnecessários estejam desabilitados: IGP (OSPF), RA IPv6, MNDP, CDP, BPDUs, Proxy ARP.....

Fornecedores de Trânsito

Solicite sempre full route e filtre os recebimentos de prefixos de seu upstream, de acordo com sua engenharia de tráfego.

Filtro de Cliente

Deve-se aceitar apenas os prefixos que foram designados por você ao cliente, pelo NIC.br ou por um RIR.

Peers

Nas interfaces com sessões eBGP é importante que todos os serviços e protocolos desnecessários estejam desabilitados: IGP (OSPF), RA IPv6, MNDP, CDP, BPDUs, Proxy ARP.....

Fornecedores de Trânsito

Solicite sempre full route e filtre os recebimentos de prefixos de seu upstream, de acordo com sua engenharia de tráfego.

Gestão do Bloco de ips

Na página de gerência de ASN é possível:

Configurar os dados de AS-IN e AS-OUT
obedecendo a RFC 1786;

Configurar a delegação de DNS Reverso;

Designar os blocos para clientes /29 e/ou
/48 em diante.

**OBS: O Registro.br utiliza os dados de blocos
delegados como ferramenta de avaliação em
uma eventual solicitação de novos blocos.**

EPP

Extensible Provisioning Protocol

O Registro.br oferece um sistema de provisionamento chamado EPP, bem como uma biblioteca chamada libepp-nicbr.

Com o EPP é possível automatizar a gerência dos recursos de numeração (bem como dos nomes de domínio), integrando-a aos sistemas internos de provisionamento e controle do provedor.

<http://registro.br/epp/>

registro.br

Registro de Domínios
para a Internet no Brasil

EPP

Extensible Provisioning Protocol

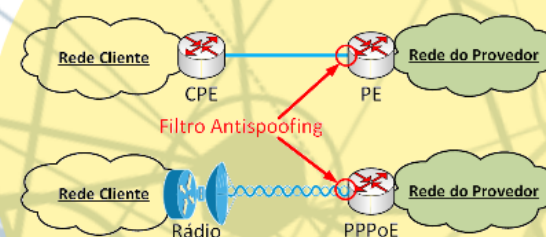
O Registro.br oferece um sistema de provisionamento chamado EPP, bem como uma biblioteca chamada libepp-nicbr.

Com o EPP é possível automatizar a gerência dos recursos de numeração (bem como dos nomes de domínio), integrando-a aos sistemas internos de provisionamento e controle do provedor.

<http://registro.br/epp/>

AntiSpoofing (RFC 287)

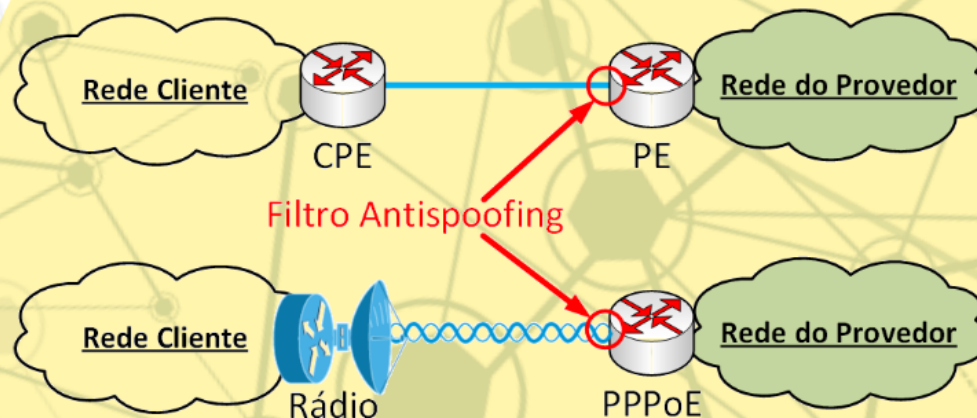
Pacotes IP com endereços de origem incorretos podem ser gerados e utilizados. Isso é spoofing, ou falsificação de pacotes. Qualquer rede na Internet pode ser vítima desse tipo de ataque.



Solução

A RFC 287 recomenda que se filtrem pacotes na interface de entrada da rede do provedor, de forma a permitir somente aqueles cujo endereço de origem seja parte da rede conectada àquela interface.

<http://bcp.nic.br/filtro-antispoofing-exemplo-para-mikrotik/>

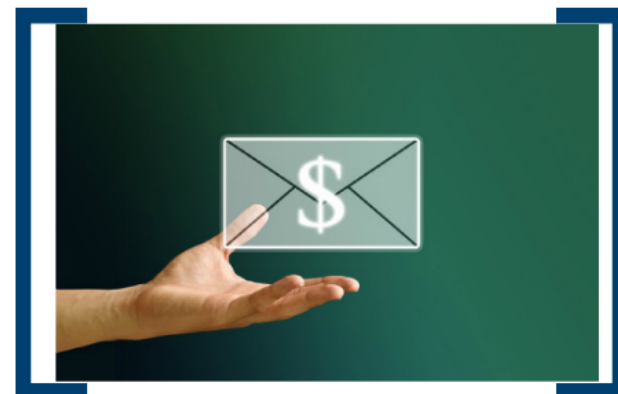


Solução

A RFC 287 recomenda que se filtrem pacotes na interface de entrada da rede do provedor, de forma a permitir somente aqueles cujo endereço de origem seja parte da rede conectada àquela interface.

<http://bcp.nic.br/filtro-antispoofing-exemplo-para-mikrotik/>

Gerência da Porta 25



Provedores de serviços de correio eletrônico.

**Mas o que é gerência de porta 25?
É o conjunto de ações, aplicadas em redes residenciais, para separar a submissão de e-mails por um usuário, do transporte de mensagens entre servidores de e-mail. A submissão de e-mails, feita via softwares como Thunderbird e Outlook, passa a ser por uma porta exclusiva para esse fim: a 587/TCP, com autenticação. Já o transporte continua sendo feito via 25/TCP.**

<http://antispam.br>

SPAM

Um problema que afeta a todos mas que não diz respeito a todos.

Provedores Acesso a Internet.

Em redes de usuários finais, de caráter residencial, recomenda-se que sejam implementadas restrições para impedir a entrega direta de mensagens a partir de máquinas clientes, através do bloqueio do tráfego de saída para a porta 25/TCP.

Provedores Acesso a Internet.

Em redes de usuários finais, de caráter residencial, recomenda-se que sejam implementadas restrições para impedir a entrega direta de mensagens a partir de máquinas clientes, através do bloqueio do tráfego de saída para a porta 25/TCP.

SPAM


**Um problema que
afeta a todos mas
que não diz respeito
a todos.**

NTP - Network Time Protocol

Protocolo de Tempo para Redes

- Apoia processos de detecção de incidentes de segurança e seu tratamento adequado, permitindo a correlação de eventos;
- A documentação e preservação de evidências que possam vir a ser utilizadas em investigações de crimes de informática.
- Gerar registro de eventos (logs) pertinentes, de forma a manter informações inequívocas sobre o fuso horário em que se deu um evento.

<http://ntp.br>



O IRR é um sistema global de bases de dados que armazenam e compartilham informações sobre políticas de roteamento. Foi desenvolvido com o objetivo de promover estabilidade, consistência e segurança ao roteamento global. No Brasil temos este serviço gratuito e de fácil configuração em:

<http://www.bgp.net.br/br/wizard>

IRR - Internet Routing Registry

RPKI - Resource Public Key Infrastructure

RPKI é uma infra-estrutura que combina a hierarquia do modelo de designação de recursos da Internet através de Registros Regionais (RIRs) com o uso de certificados digitais baseados na norma X509.

O LACNIC participa na definição dos padrões que hoje permitem o desenvolvimento dessa ferramenta e desde janeiro de 2011 encontra-se em produção o Serviço de Certificação de Recursos do LACNIC.

<http://rpki.lacnic.net/>

Algumas Aplicações

- Construção de filtros para anúncios usando BGP.
- Construção de regras de roteamento baseadas na validade criptográfica dos prefixos anunciados.
- Extensões de segurança para IGP, como OSPF ou ISIS.
- Autenticação de rotas nas redes de área local.
- Assinatura de informação em serviços de Whois ou em objetos RPSL (Routing Policy Specification Language).

Algumas Aplicações

- Construção de filtros para anúncios usando BGP.**
- Construção de regras de roteamento baseadas na validade criptográfica dos prefixos anunciados.**
- Extensões de segurança para IGP, como OSPF ou ISIS.**
- Autenticação de routers nas redes de área local.**
- Assinatura de informação em serviços de Whois ou em objetos RPSL (Routing Policy Specification Language).**

Team Cymru

Equipe Cymru

é uma empresa de pesquisa de segurança na Internet especializada, sem fins lucrativos, dedicada a tornar a Internet mais segura, ajudando os ASN a identificar e erradicar os problemas em suas redes, fornecendo informações de IPs que ainda não foram alocados pelos seus RIR.

<http://www.team-cymru.org>



TEAM CYMRU NFP
INSIGHT THAT IMPROVES LIVES
<https://www.team-cymru.org/>

LOG x Monitoramento

"O que não pode ser medido não pode ser Gerenciado" W.E. Deming

LOG

- Um log é um arquivo que grava informações de eventos possuindo diversas utilidades, incluindo a descoberta de problemas, detecção de invasão, gerenciamento de operações e usuários, além da análise forense quando necessário.
- Um padrão de log é o syslog criado pelo IETF (RFC 5424) que utiliza o protocolo UDP na porta 514.

Monitoramento

O protocolo SNMP RFC3584 - É o protocolo de gerência de rede, que possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver seus eventuais problemas, e fornecer informações para o planejamento de sua rede.



DISCIPLINA X CONTROLE



The Dude

SpamHaus - BGPf

BGPf Advisory Null Route

Spamhaus oferece uma sessão BGP de três das suas listas.

Lista Botnet C&C, DROP e DROP estendida (EDROP).

Estas listas são usadas para bloquear os pacotes provenientes de IPs envolvidos em certos tipos de atividade maliciosa.

Spamhaus BGP feed (BGPf)

Community	Name	Notes	Pricing
65190:1000	Spamhaus DROP	Serves Spamhaus DROP list	annual
65190:2000	Spamhaus EDROP	Serves Spamhaus extended DROP list	annual
65190:3000	Spamhaus BGPCC	Serves Spamhaus Botnet C&C list	annual

<http://www.spamhaus.org/bgpf/>



EQUIPE

The diagram features a central yellow circle with a dark blue border. To the left, a yellow banner with the word 'EQUIPE' in bold black letters points to the center. To the right, four yellow circles with dark blue borders are connected to the central circle by dark blue lines. The background is a light blue network of lines and hexagons.

Grupo de pessoas com habilidades complementares, que trabalham juntas com a finalidade de atingir um propósito comum; pelo qual se consideram coletivamente responsáveis.

Respeito, treinamento, reconhecimento, metas, confiança, oportunidade e cooperação, são as ações de lideranças para obter uma excelente equipe.

Aprendizado

Exemplo

Ambiente Saudável

Fazer o que gosta

EQUIPE



• www.youtube.com/watch?v=raO2V5oBVB4

CONCLUSÃO....

Um AS Saudável é muito mais que seu BGP, normas e regras. É promover um bom ambiente de trabalho e motivar a equipe a prestar um serviço de qualidade, seguro, estável, transparente, ético, justo para o cliente e rentável para a empresa.



Obrigado!!!

Lacier Dias
lacier@titania.com.br
Skype: lacier.dias
(65) 9968-5684



