**SR. ANTÔNIO MARCOS MOREIRAS**: Olá, muito bom dia a todos. Muito boa semana, porque essa semana vai ser bastante especial. A gente está promovendo a Semana de Capacitação On-Line do NIC.br. E, durante essa semana inteira, começando hoje, segunda-feira, até sexta, das 9h ao meio-dia, a gente está trazendo tutoriais técnicos para vocês. Tutoriais técnicos voltados para comunidade técnica de internet e redes aqui no Brasil.

E, hoje, a gente tem um tutorial promovido pelo próprio NIC.br. A equipe do Ceptro, a Erina, o Eduardo e o Tiago vão trazer para vocês um tutorial fantástico sobre RPKI, uma atualização do tutorial que já foi dado no final do ano passado. Agora já trazendo a interface gráfica do RPKI, muita coisa interessante. E nos demais dias a gente tem a participação de parceiros, né? Empresas que toparam ajudar a gente trazendo informação de qualidade para toda a comunidade técnica. Então a gente vai ter a Cisco trazendo assunto segurança para provedores. A gente vai ter a Icann trazendo o assunto DNS, DNSSEC.

A gente vai ter a VLSM falando de anúncios BGP, de automatização com Huawei e Mikrotik. E a gente vai ter a Juniper e a Wztech falando sobre L2, sobre Ethernet na sexta-feira. É legal lembrar até que a gente está promovendo também uma série de lives chamada Intra Rede.

Na última live que a gente teve o Daniel Fink, da Icann, esteve lá falando sobre DNS. Ele falou justamente da importância do DNSSEC, da importância do DNS recursivo, da importância do Hyperlocal. E agora ele vem aqui, na quarta-feira, trazer o tutorial sobre como fazer isso, né? Então estou linkando a coisa aqui para vocês verem que o assunto é importante. E a gente vai trazendo diversos conteúdos complementares dentro dessas lives que a gente vai fazendo. Da mesma forma, a gente vai ter a próxima live do Intra Rede em 30 de setembro falando sobre segurança. Então vocês já anotem aí na sua agenda: 30 de setembro, segurança, o assunto.

E aproveitando, falando de anotar na agenda, né? A gente tem um pouco mais de 370 pessoas assistindo agora. E tem um potencial para ter muito mais. Está cedo ainda, o pessoal está acordando, então, aproveita aí, gente. Manda o link da transmissão. Eu já vou deixar o Eduardo, a Erina e o Tiago entrarem no assunto técnico, começarem o tutorial. Mas enquanto isso, dá o like no vídeo para Youtube passar, para o Youtube passar isso na timeline de todo mundo que assina o canal. Quanto mais likes mais o Youtube faz a distribuição orgânica, mais ele mostra esse vídeo para quem é assinante do canal.

E repassa aí, o link do vídeo no seu grupo de Whatsapp. Não precisa repassar no grupo da família, mas no grupo dos provedores, no grupo do pessoal técnico, tal, repassa, chama o pessoal para assistir essa live. E avise. Mesmo que o pessoal perca a live agora, vai ficar gravado imediatamente aí no YouTube.

Antes ainda de deixar o Eduardo, o Tiago e a Erina falarem, eu preciso lembrar de vocês de algumas coisas importantes que aconteceram aí nos últimos dias, né? E comentar com vocês.

Uma delas foi o final do IPv4, né? Como assim, Moreiras? O IPv4 já não tinha acabado lá em 2014? O NIC.br falou que IPv4 acabou lá em 2014, e agora você está falando do final de IPv4 de novo essa semana?

É isso mesmo! A comunidade técnica decidiu que haveria uma espécie de uma reserva, que a gente chamou de reserva de esgotamento gradativo, né? Foi uma reserva para novos entrantes. Que, de 2014 até agora, ela foi distribuída justamente para os novos entrantes, para o pessoal que nunca tinha pedido uma locação de IPv4 antes para o Registro.Br, ou para o Lacnic ou NIC México aqui na América Latina. E essa reserva terminou. A gente não tem mais.

Agora vai ser feito... agora tem uma fila, e, se houver recuperação de algum endereço pode até ter alguma locação de IPv4 pelo Registro.Br. Mas não tem mais estoque. O Lacnic não tem mais estoque, o Registro.Br não tem mais estoque de IPv4. Então chegou a hora, né? Acabou finalmente o que a gente vinha falando aí, há muitos anos já, de fato aconteceu.

E é uma deixa aí, forte para quem não implantou IPv6, não começou a implantação do IPv6 ainda, levar isso a sério. Começar a implantação do IPv6. IPv6 é o caminho para o futuro da Internet. O IPv6 já é considerado o protocolo atual da Internet. Todos os demais protocolos, todo o desenvolvimento de protocolos que acontece, né? Os, vamos dizer assim, upgrades nos protocolos, as modificações, as melhorias nos protocolos que acontecem lá no IETF, as novas RFCs, todas são feitas em cima do IPv6. O IPv6 é considerado o protocolo atual da Internet. A gente tem mais já do que 30% de usuários de Internet com IPv6 ativo.

Então se o seu provedor ainda não entrega IPv6 para o usuário final, vai atrás, né? Ah, é um caminho sem nenhum problema? Não tem nenhuma pedra no meio do caminho? É fácil? Mamãozinho com açúcar colocar IPv6? Olha, tem problemas, não é impossível, não é difícil. A gente tem cursos gratuitos, tem muito material técnico disponível, tem cursos por aí no mercado. Tem equipamentos que suportam o IPv6, e tem muitos provedores iguais ao seu que já fizeram, né? Então se os outros fizeram, você também consegue. Então vá atrás!

E uma outra coisa que eu gostaria de comentar, não poderia deixar de comentar, é que semana passada o IX.br/São Paulo, PTT de São Paulo, alcançou a marca dos 10 terabit por segundo, ultrapassou a marca dos 10 terabit por segundo de pico. E foi a primeira vez que o Internet exchange no mundo chegou nos dois dígitos, em 10 terabits. Então, isso faz do IX.br/São Paulo, do PTT de São Paulo, o maior Internet exchange do mundo! Tanto em tráfego quanto em número de redes conectadas. Isso, para a gente, é algo a se comemorar. É um grande feito para a gente. Então a gente está muito feliz com isso daí.

Por fim, eu já vou chamar o pessoal para entrar no assunto técnico. Eu quero mostrar para vocês um vídeo bem curto, bem pequenininho, um vídeo de 15 segundos. Que é de um projeto que a gente está trabalhando, né? Um projeto que a equipe do Eduardo, a equipe que cuida aqui desses cursos, desses eventos técnicos dentro do Ceptro, está preparando para comunidade.

É um projeto que vai trazer dicas técnicas para o usuário leigo. E que a gente espera que em breve a gente possa lançar. A gente está trabalhando nos vídeos, e eu vou mostrar esse para vocês como um teasing, como uma mostra do que vem aí pela frente. Tá bom?

Pedro, se você conseguir colocar o videozinho agora, fica à vontade. Não tem som, são só 15 segundos de vídeo. E, depois do vídeo eu nem vou voltar a falar aqui, o Eduardo, ou o Tiago, ou Erina, não sei quem vai começar o tutorial, eles vão assumir.

[exibição de vídeo]

**SR. EDUARDO BARASAL MORALES**: Bom dia a todos. Sejam todos bem-vindos à primeira semana de capacitação do NIC.br. Um projeto que a gente criou esse ano, justamente para trazer um conhecimento técnico para os sistemas autônomos, os provedores e os administradores de redes. Então, não percam os conteúdos que a gente vai apresentar essa semana.

No dia de hoje, a gente vai ter uma palestra sobre RPKI. Apresentando ali como trabalhar com esse novo sistema.

Depois, nos demais dias, a gente vai ter a parceria com algumas empresas de conteúdo. Então teremos Juniper, Wztech, Icann, VLSM e Cisco. Cada uma delas apresentando ali, em um determinado dia, um conteúdo técnico só para vocês. Então não percam os próximos dias aí, relacionados à nossa semana de capacitação.

Bom, como eu já tinha falado, no dia de hoje vamos apresentar segurança no roteamento com RPKI.

Para aqueles que não sabem, o sistema ali do RPKI existe há muito tempo, só que aqui no Brasil o sistema e a permissão de você trabalhar com RPKI só foi possível no final do ano passado, quando o Registro.Br conseguiu implementar o RPKI para os sistemas autônomos brasileiros. Tanto que na semana de infraestrutura, quando foi lançada essa questão do RPKI, a gente fez um tutorial técnico de oito horas só sobre esse assunto. E hoje, aqui, a gente vai ter três horas para abordar o assunto de RPKI. Então vai ter como se fosse uma atualização de parte do conteúdo que a gente apresentou no ano passado.

E como que a gente está estruturando apresentação no dia de hoje? Bom, primeiramente, para quem não me conhece, meu nome é Eduardo Barasal Morales, e, junto com a minha equipe, eu vou apresentar aqui para vocês um pouco sobre o RPKI. Então a gente vai ter Andrea Erina Komo e o Tiago Jun Nakamura apresentando em conjunto o RPKI.

Como que estruturamos a nossa conversa de hoje? Primeiramente a gente vai fazer um nivelamento de conhecimento, falando sobre roteamento de BGP, vulnerabilidade e segurança. Que é a motivação da criação do RPKI. Depois disso a gente vai falar sobre um projeto muito interessante para os sistemas autônomos, que é o MANRS. Adentraremos em conceitos de segurança, criptografia e certificação digital. E aí vamos falar sobre o RPKI. Sobre componentes do RPKI, como participar e os anúncios de suas rotas no RPKI. E, no final, vamos também falar sobre a segunda parte do RPKI, que é a questão de validação da origem. Só que esse conceito ele é muito amplo, não dá para a gente abordar aqui tudo em três horas. Então a parte prática que a gente vai se focar mais vai ser a questão de publicação dos ROAs, dos anúncios das nossas notas rotas no RPKI. A questão de validação a gente vai deixar um pouquinho mais para frente em um outro tutorial. Então, por hoje, a gente vai focar muito mais na parte de publicação.

Então, entrando em conceitos de roteamento, para dar aquela nivelada básica. O que é BGP? Que é a base para a gente poder falar sobre o RPKI.

Bom, BGP para quem não sabe, é o Border Gateway Protocol, é um protocolo de roteamento, que vai ali passar rotas entre sistemas autônomos, né? Então, é assim que a gente está olhando nessa imagem, você vai ver que a Internet é composta por diversos sistemas autônomos. Cada sistema autônomo tem ali os seus blocos de endereço IPv4 e IPv6, que vai colocar nas máquinas, nos seus clientes, assim por diante, e vai criar os caminhos, que são as rotas. E essas rotas tem que ser propagadas para os sistemas autônomos, como está mostrando as setinhas ali, em vermelho. Então ela vai divulgar essa informação e vai repassar entre os sistemas autônomos.

É assim que a Internet funciona. Depois que todo mundo conhece as rotas, a comunicação, ela acontece lá da origem até um determinado destino.

Então é importante a gente ter esse conceito do sistema autônomo e do BGP, que vai trafegar as rotas de um Sistema autônomo para o outro.

O BGP, tá? Ele é usado no backbone da Internet por todos os sistemas autônomos. Então se o sistema autônomo quer adentrar na Internet, ele precisa conversar BGP com os outros Sistemas autônomos. E o

BGP, ele é um protocolo que é baseado na confiança. Tanto que o que você informa através do BGP o outro aceita.

Então se você está enviando informações corretas, o outro lado está aceitando informações corretas. Mas se você está mandando informações erradas, o outro lado também está aceitando as informações erradas. Então é por isso que a gente tem que tomar muito cuidado com o BGP, porque ele trabalha muito na questão de confiança.

E, além de trabalhar na questão de confiança, ele é um protocolo baseado em fofoca. Ou seja, o que você informa para um sistema autônomo, ele vai repassar para outro sistema autônomo, que vai repassar para outro sistema autônomo, que vai repassar para outro sistema autônomo e assim por diante na Internet. Então o que um aprende vai repassando para os outros. Então ele é baseado em confiança e baseado em fofoca também. E é um protocolo político, né? Tanto é que a gente fala que você tem que implementar as políticas de tráfego.

Então você tem que conversar com outro sistema autônomo e ver o que ele vai aceitar. E falar para ele o que ele vai te mandar para você colocar filtros, para você colocar ali suas melhores políticas de tráfego, tá? para você aceitar o melhor caminho e definir ali a sua melhor rota.

Então o BGP, ele é um protocolo que é político, fofoqueiro e baseado em confiança. Então por isso que a gente tem que tomar muito cuidado. Mas a Internet funciona dessa forma.

E quais são os problemas de segurança em roteamento? Então vocês podem ter visto aí, cada vez mais está surgindo aí, nos noticiários, né, problemas relacionados à Internet. Problemas de segurança. Então como roubo de prefixo, uma parte da Internet fica fora, um provedor fica fora, um provedor de conteúdo grande, né? Como aí está mostrando, o Google ficou fora. Ou causando ali que o Japão fique fora, mostrando ali um pouquinho ali das notícias. Então a gente tem cada vez mais vendo ataques e ataques na Internet, e por isso a gente tem que tomar cuidado com a Internet. Porque o impacto pode ser muito grande. Principalmente que agora que a sociedade depende muito da Internet.

Tanto que uma das coisas que a gente gosta de ressaltar para os nossos alunos é que não existe nenhum dia sequer sem incidentes na Internet. Então vocês podem dar uma olhada aí no gráfico, depois podem entrar no site do bgpstream.caida.org. E vocês vão ter todos incidentes que estão acontecendo em determinado momento, tanto no passado, como também agora. Então vocês podem ver que não existe ali nenhum dia sequer sem atividades suspeitas na internet. Com uma possibilidade de roubo de prefixo, de um vazamento de prefixo. Tudo isso daí acontecendo na internet e afetando os provedores, tanto de conteúdo, como provedores de internet. Então afeta ali, o sistema como um todo.

Mas lembra, isso acontece porque o BGP aceita muita coisa. Ele trabalha com a confiança. Então faz algum erro, o impacto ali pode ser ali catastrófico, pode afetar muita gente. Então por isso que a gente tem que tomar cuidado.

Então por que isso acontece? Então, lembrando que a gente mostrou naquele slide que várias nuvenzinhas ali se comunicando, que a gente chamou de sistemas autônomos e elas trocando rotas entre si através do BGP.

Bom, a internet é uma composição dessas nuvenzinhas de sistemas autônomos, que a gente pode dizer ali que são mais de 60 mil sistemas autônomos espalhados pelo mundo todo.

E cada sistema autônomo tem autonomia sobre o seu BGP, sobre o que vai anunciar e sobre o que vai receber. Então ele pode filtrar, ele pode ali, anunciar as coisas mais específicas, menos específicas e trabalhar ali, da melhor forma como que é o seu tráfego.

Só que, lembra? É um sistema que todos dependem de todo mundo para funcionar. Então fez uma besteira, o impacto é propagado para todo mundo, e aí a gente tem ali um grande problema. Por quê? Porque o roteamento, ele trabalha com cooperação e confiança. Então não tem validação de dados por default ali no BGP. Então, fez besteira, está propagando aquela besteira.

Mas quais são as besteiras que a gente pode falar ali do BGP, né? Que tanto podem afetar ali os provedores? Um dos principais deles é a questão do BGP Hijacking, ou seja, anúncio de prefixos não autorizados, que o pessoal chama de: sequestro de prefixo.

Então você tem ali um determinado bloco IPv4, um determinado bloco IPv6. Então você tem ali aquele bloco para criar rotas. E aí você manda para internet aquelas suas rotas determinando o seu bloco. Mas, porventura, pode acontecer de outra pessoa anunciar o seu bloco. Mas por que alguém anunciaria o seu bloco, né? O que caracterizaria um sequestro de prefixo. Bom, pode ser um erro de configuração. Ele digitou ali o bloco errado no roteador, e aí passou aquilo adiante. Então é um dos problemas.

Depois disso, tem ali o fat finger, né? Que a gente chama ali do 'dedo gordo'. Então, ele queria clicar no botão sete, mas o dedinho gordo dele foi até o número oito, e aí colocou uma nova rota, um novo prefixo ali, que vai ser anunciado. E aí ele acaba roubando, sem querer, o prefixo de um outro sistema autônomo.

Mas o problema principal está o quê? Na maneira proposital, ou seja, a intencional de roubar um prefixo. Então aí ele está pensando ali talvez em prejudicar um outro sistema autônomo. E é isso tudo que a gente vai querer evitar, tá? Na questão aí, do problema de BGP Hijacking.

Então vamos olhar aí, através de um exemplo, né? A gente tem aqui o AS 65536 que quer mandar um pacote para o 2001 db8 1. Bom, para ele mandar esse pacote, ele precisa de uma rota. Quem que é o dono dessa rota? Aí ele vai ver lá na sua tabela de roteamento que existem duas entradas: a 2001 db8/32, indo para o 65537, e o 2001 db8/48 indo para o 65540. Os dois estão ali divulgando aquela rota. Só que, na verdade, só um deles é dono daquele bloco, que no caso é o 65537. Então, o 65536, tendo essas duas rotas, qual que ele escolhe? Aí, pessoal, ele vai acabar escolhendo o quê? A rota mais específica, que é o quê? O /48. Mas, afinal, o /48 está indo para o verdadeiro dono do bloco? No nosso desenho aqui não. Foi um outro Sistema autônomo que anunciou aquela rota mais específica, que pode ter sido ali um erro. Mas ele acabou roubando o tráfego, que, afinal, ele divulgou uma rota mais específica. E você, aceitando aquela rota você vai encaminhar o seu tráfego por aquele caminho.

Mas vamos dar uma olhada na questão do problema dois. A gente tem ali os mesmos sistemas autônomos, o 40 divulgando o /32 e o 37 divulgando também o /32. Agora eles estão divulgando a mesma rota. Só que um dá um salto a mais. Por quê? Porque ele tem um provedor no meio do caminho, o 65544. E, por sinal, é o caminho do verdadeiro.

Olhando as duas rotas o BGP, ele tem que tomar uma decisão. No caso ele vai escolher o quê? O caminho mais curto. Que, no caso, é o falso dono. Então novamente essa é uma outra situação de roubo de tráfego usando, às vezes, o mesmo prefixo.

O que eu quero ressaltar aqui? No primeiro, com a rota mais específica, a decisão foi do roteador. Aqui a gente está trabalhando com decisão do BGP. O caminho mais longo de AS, o BGP vai dizer qual vai ser a melhor rota. Então o caminho mais curto vai ainda ser para o falso dono.

Então perceba que um provedor que divulga uma coisa errada, seja de maneira proposital ou de maneira errada, ele prejudica a internet. Ele prejudica ali o verdadeiro dono, porque ele está roubando o tráfego.

Mas, assim, roubar o tráfego não quer dizer que é uma coisa boa. Lembra? Ele também contrata links de trânsito. Então está consumindo link de trânsito dele. Então pode ser que ele fez aquilo errado e ele está se prejudicando também.

Mas como resolver esses problemas? Bom, aí é legal de a gente comentar de um projeto chamado MANRS, Mutually Agreed Norms for Routing Security, ou o anacrônimo de MANRS, que, na verdade, é um jeito de você falar que você tem good manrs, boas maneiras na internet na questão ali de roteamento.

É uma iniciativa global, que foi, ali, com apoio da Isoc chegar nos sistemas autônomos para que eles consigam fazer ali boas práticas de segurança em roteamento. E ele consiste em quatro ações básicas: filtro, anti-spoofing, coordenação e validação global.

E um desses tópicos entra o RPKI. Por isso que a gente tá falando desse projeto. Ele engloba mais coisas, outros problemas além do roubo de prefixo e vazamento de rotas, que é importante a gente ver os sistemas autônomos participando, para a gente ter ali uma internet melhor para todo mundo. mas ele também inclui o RPKI.

Então olhem esse projeto, façam ali os tutoriais e se inscrevam. Tá? Se todo mundo fizer a sua parte, a internet melhora para todos. Então é importante ser um bom cidadão na internet.

Então aqui a gente tem o site do projeto, do manrs.org. Então você pode assinar o projeto e solicitar que os seus clientes e upstreams também assinem o projeto. Se todo mundo assinar, melhora para todo mundo. E o RPKI tá lá dentro, é um dos tópicos. Então, agora que você vai aprender o RPKI nesse tutorial, você vai, depois, poder assinar por completo o MANRS. Fazendo ali todas as práticas corretas, tá?

Então vamos lá. O que é o RPKI? RPKI é o Resource Public Key Infraestructure, tá? Então é uma infraestrutura de chaves públicas, né? para questão ali dos recursos. No caso que a gente está falando de recursos, são ali os blocos IPv4, os blocos IPv6, os sistemas autônomos, que a gente vai poder utilizar essa informação para gerar uma rota.

Então ela é uma estrutura desenvolvida para validar os recursos de numeração, ASN e os prefixos IPs que a gente vai utilizar no BGP. E isso vai evitar ali os problemas de BGP Hijacking, principalmente aqueles que o cara clicou errado, configurou errado, teve ali o dedinho gordo, clicou no botão errado. Isso daí vai melhorar para todo mundo.

Aquelas de medida intencional que a pessoa quer fazer ali, um ataque em determinado sistema autônomo, vai ali ajudar, mas, sabe, quando alguém quer fazer alguma coisa para prejudicar o outro, existem inúmeras outras maneiras. Então isso daí não vai prevenir todos os problemas. Vai, assim, melhorar. Mas se todo mundo fizer isso, melhora para todos os sistemas autônomos. Por isso que a gente fala que a colaboração é essencial.

Então vamos ver ali o exemplo do RPKI. A gente tinha aquele exemplo problema, que ele queria mandar um pacote para um determinado dispositivo, o 65536. E ele tinha ali recebido as duas rotas. Então, lembrando ali, rota mais específica e a menos específica.

Só que agora a gente tem o RPKI dizendo quem que é o dono verdadeiro, qual que é a rota válida. E aí você vai poder marcar essa rota e descartar a rota inválida.

Então nesse caso, mesmo recebendo o mais específico, se ele não é o verdadeiro dono, não tiver assinado aquela rota, você vai poder descartar e ficar só com a verdadeira. E logo o seu tráfego vai chegar no lugar certo. Então perceba que o RPKI vai te dar essa segurança, essa tranquilidade.

Então falando ali de conceitos de segurança. E agora eu vou passar para Erina, que ela vai explicar toda essa questão de publicação dos ROAs, que vai permitir que o seu bloco seja ali, demarcado por quem pode utilizar para propagar uma rota. E isso vai dar uma segurança para você que vai evitar que outros roubem a sua rota.

Então, Erina, fique à vontade.

**SRA. ANDREA ERINA KOMO**: Oi, pessoal, eu sou Andrea Erina Komo. E, conforme o Eduardo disse, né? Vamos ver agora alguns conceitos de segurança. Esses conceitos vão ser importantes para a gente entender mais para frente como é que funciona essa parte de segurança no RPKI.

Existem diversos aspectos que caracterizam segurança em um sistema de computadores. Esses aspectos, né, são conhecidos como serviços de segurança.

Existem cinco serviços básicos de segurança que é importante a gente conhecer. Então vamos ver quais são eles.

O primeiro listado ali, no nosso slide, é disponibilidade. Essa característica de manter uma aplicação ou um serviço sempre acessível para os usuários legítimos desse sistema. Um exemplo aí de um sistema que requer alta disponibilidade são os servidores DNS.

Seguindo ali na nossa lista, o próximo é confidencialidade. Acredito que esse é um pouquinho mais conhecido. É a ideia de manter uma informação secreta, confidencial, criptografada. Isso é, apenas os usuários autorizados podem ter acesso à essa informação.

Junto dele a gente também colocou ali privacidade, que está relacionado, com essa ideia de confidencial, só que, ao invés de confidencializar ali alguma informação em geral, o importante é deixar confidencial a identidade do usuário. Então, os dois estão relacionados.

O próximo é integridade. O objetivo desse serviço é garantir que uma informação não sofreu qualquer tipo de alteração, seja proposital ou acidental.

O próximo é autenticidade. A ideia da autenticidade é você ter certeza do autor, da fonte de uma determinada informação. Então, por exemplo, o marido chega em casa, encontra um bilhete escrito: "Fui ao mercado comprar a janta, volto logo. Beijos". Ao ver esse bilhete, o marido sabe que quem escreveu ele foi a esposa dele. Então ele sabe que aquele bilhete é autêntico.

Já ali, seguindo para o próximo serviço, no caso de irretratabilidade, ele é parecido com autenticidade, mas tem um detalhezinho ali, de diferente. A ideia da irretratabilidade é também ter certeza ali do autor, ou da fonte de uma determinada informação, só que, além disso, você consegue comprovar quem é esse autor

para uma outra pessoa. Então, por exemplo, um documento ali assinado e com firma reconhecida. Você tem certeza de quem assinou aquele documento e você consegue ainda comprovar para as outras pessoas quem assinou esse documento a partir dessa assinatura.

Aí, onde é que está a diferença entre as duas situações da autenticidade com irretratabilidade?

Note que no meu exemplo aí, de autenticidade, o marido sabia que o bilhete era da esposa, mas ele não consegue comprovar isso, por exemplo, para um vizinho. O vizinho vai olhar aquele bilhete e não sabe quem é o autor. Pode ter sido a esposa da pessoa, assim como pode ter o marido escrito aquele bilhete e mostrado para o vizinho. Já no caso do documento assinado com firma reconhecida não tem como, né? Todo mundo sabe quem é que assinou, tem até a firma reconhecida para garantir isso. Então todo mundo tem a certeza ali de quem é o autor daquela informação, daquela assinatura. Por isso, né, que os dois são diferentes.

Bem, desses cinco serviços de segurança, disponibilidade é um serviço que não tem como você conseguir por algum algoritmo computacional. Não tem nenhum software que impeça que alguém corte o cabo de energia da rua. Então, para ter esse serviço geralmente a gente usa algum tipo de redundância.

Já os outros serviços, confidencialidade, integridade, autenticidade e irretratabilidade, existem lógicas matemáticas, algoritmos criptográficos que garantem computacionalmente esses serviços.

Então vamos ver como é que funciona isso. Um tipo de algoritmo existente é o de criptografia assimétrica. Essa criptografia aí é formada por duas chaves criptográficas distintas, mas relacionadas. Então, a gente tem uma chave pública, que seria um código aí, uma informação amplamente conhecida; e uma chave privada, que é um segredo aí, do dono dessa chave.

Então, fazendo aí uma analogia, suponha que é um par de chave/cadeado. Onde o cadeado, a informação seria pública, a chave pública, você coloca ali o cadeado, ele fica exposto e visível para qualquer um. Já a chave que abre esse cadeado, seria aí, a informação secreta, o segredo ali, que o dono dessa chave mantém guardado.

Uma característica importante aí, desse tipo de criptografia é: Toda transformação ali matemática, lógica, matemática feita usando uma chave, só pode ser desfeita usando a outra chave correspondente. Então vamos ver como assim, né? Como é que funciona isso.

Então ali no exemplo, né? Suponha que Alice quer mandar uma informação, uma mensagem secreta ali para o Bob. Aí ela decidiu fazer isso usando ali um algoritmo de criptografia assimétrica. Como que é o processo, então? Ela vai escrever ali a mensagem dela, e usar ali o algoritmo para cifrar essa mensagem. Para cifrar essa mensagem, ela vai precisar também fornecer ali a informação da chave pública do Bob. Que é para quem ela quer mandar a mensagem secreta. Ela vai juntar suas informações ali no algoritmo de cifração e, com isso, ela vai ter ali a mensagem criptografada. Ela faz o envio normal dessa mensagem criptografada, vai passar pela rede. E, ao chegar ali no Bob, o Bob vai usar a chave privada dele para decifrar aquela mensagem e ler, né? O recado ali secreto que a Alice mandou para ele.

Então, nota que a Alice usou a chave pública do Bob para cifrar e, para desfazer essa transformação, o Bob teve que usar a chave privada dele para fazer ali, a decifração.

Então, conforme eu disse, a transformação que uma chave faz a outra desfaz. Como Bob é o único que tem acesso à chave privada dele, apenas ele vai conseguir decifrar aquela mensagem. Por isso que a gente tem confidencialidade nesse sistema.

Seguindo ali uma outra situação, né? A Alice, no caso, quer gerar um documento, e ela quer conseguir comprovar que foi ela mesmo quem gerou aquele documento. Como é que ela pode fazer isso? Ela também pode usar um algoritmo ali, de criptografia assimétrica para assinar digitalmente esse documento.

Então o que ela faria? Ela geraria ali o documento que ela quer. Ela usaria ali a chave privada dela para assinar digitalmente esse documento. Esse documento assinado pode ser enviado para o Bob, e o Bob vai conseguir verificar aquela assinatura usando a chave pública da Alice. Se a verificação bater, ele tem a certeza que aquele documento foi mesmo gerado pela Alice.

Então, aqui no caso, o processo começou usando a chave privada, ele foi feito ali usando a chave privada, e aí ele foi desfeito usando a chave pública. Então, como apenas a Alice é dona daquela chave, apenas a Alice consegue fazer aquela assinatura. Por isso que a gente tem a certeza de que aquela mensagem, aquele documento veio da Alice. Então a gente tem autenticidade. Como qualquer um, que tenha a chave pública da Alice consegue fazer aquela verificação. Então qualquer um consegue ver que aquele documento foi assinado pela Alice. Tanto o Bob, quanto uma outra pessoa consegue verificar isso. O Bob consegue comprovar isso para qualquer outra pessoa. Então a gente também tem ali a parte da irretratabilidade.

E, esse sistema também garante integridade, porque se tiver qualquer alteração ali no meio do caminho, se, porventura, durante ali a transmissão do documento assinado teve algum problema, quando for feita a verificação, a informação não vai bater. Então a assinatura não vai estar correta. Aí também garante integridade por isso. A gente consegue identificar se tiver qualquer alteração em relação ao documento originalmente assinado. Por isso que a assinatura digital fornece para a gente irretratabilidade, autenticidade e integridade.

Um ponto importante de todo esse sistema de criptografia assimétrica é que a segurança do sistema, todos serviços de segurança aí que eu falei que ele fornece, estão em cima, estão fundamentados nas chaves criptográficas. Então toda a segurança depende ali da chave privada e da chave pública, que são usadas ali no sistema.

E aí um ponto importante, né? A gente tomar cuidado é: Como garantir a credibilidade ali, de uma chave pública? Como é que eu garanto que a chave pública que eu recebi é mesmo de quem eu acho que é? Ali, por exemplo, no caso, o Dick está se passando pelo Bob, e informando ali a chave pública dele para Alice. A Alice, acreditando que está falando com o Bob, vai usar aquela chave durante toda comunicação, e, no final, ela vai estar, na verdade, mandando as informações para o Dick e não para o Bob. Então se ela tentar ali, cifrar qualquer mensagem para o Bob, na verdade, é o Dick quem vai ler as mensagens secretas. E se o Dick gerar qualquer documento assinado por ele, ela vai achar, né, a Alice vai achar que foi assinado pelo Bob. Então toda a segurança do sistema ali foi comprometida.

Então é fundamental, é importante garantir essa credibilidade das chaves. Garantir certinho a verificação de quem é o dono daquele par de chaves.

Para isso foram criados os certificados digitais. Esses certificados são documentos que associam uma chave pública ao seu dono. Então, seguindo ali, no modelo de PKI ou ICP, infraestrutura de chave pública, o

certificado digital contém a informação do dono da chave, a chave pública dessa pessoa e esse documento, esse certificado é assinado aí por uma autoridade certificadora.

Então o certificado digital é basicamente ali a chave pública do Bob, a informação ali pessoal do Bob, por exemplo, o nome dele, falando: Ah, o dono dessa chave é o Bob. A chave é tal. E quem atesta que essa informação está correta é a autoridade certificadora. No caso ali a CA, né? Certificate Authority. E aí, com essa informação certificada, a Alice tem certeza de que a chave que ela está usando pertence mesmo ao Bob, ela não está sendo enganada dessa vez pelo Dick.

Aí, como é que funciona esse modelo de PKI que eu mencionei antes? A ideia é que existe uma cadeia de certificação. Então você tem autoridades certificadoras, CAs, que são entidades confiáveis, e que todo mundo conhece as chaves públicas dessas entidades. E aí, a partir dessas entidades amplamente conhecidas e confiáveis, é gerada uma cadeia de certificação até chegar ali, nas entidades finais da cadeia.

Então a gente tem ali um primeiro nível as entidades raiz. Aí elas geram certificados digitais para ali sub CAs. E essas sub CAs, no caso, assinam ali o certificado digital das entidades finais, as end entitys.

O que seriam esses certificados finais? Seria, no caso, aquele exemplo anterior, o certificado digital do Bob. O Bob não vai assinar o certificado para outra pessoa, ele vai ter só o certificado digital dele, atestando que ele é dono daquela chave pública. E isso é confirmado, verificado pela assinatura das autoridades certificadoras ali acima da cadeia, que foram gerando ali, até chegar no certificado dele.

Então, o A vai gerar um certificado para o C e assinar esse certificado. O C vai gerar um certificado para o F e assinar esse certificado. Você verificando a assinatura do C, no certificado do F, e verificando a assinatura do A no certificado do C, você confia que aquele certificado final que você recebeu do F é verdadeiro, é confiável. Então por isso que tem toda essa cadeia.

Então, aí um exemplo aí no caso. Como eu falei, tem o certificado da autoridade raiz, que vai gerar o certificado de uma autoridade certificadora ali intermediária, até que vai gerar o certificado ali, da entidade final.

Aí mais alguns detalhes sobre a estrutura desse modelo de PKI. Os certificados digitais gerados seguem um padrão conhecido como X509. Então, nesse certificado digital tem algumas informações presentes que eu listei. Então, só para o pessoal ter uma ideia, ele vai com uma informação ali de versão, número de série, tempo de validade, qual é a chave pública, informação do dono dessa chave, assinatura ali da entidade que está autenticando aquela informação. Então esse é o padrão usado aí, para os certificados do modelo de PKI.

E nessa estrutura de PKI a gente também tem mais um documento conhecido como CRL. O que é a CRL? É a lista de certificados revogados. Então é como se fosse uma lista negra de certificados, que tiveram algum problema, algum comprometimento na segurança deles. Então, algum problema aconteceu com a chave privada correspondente ali àquele certificado digital. Então aquele certificado já não é mais seguro você confiar naquela informação, não é mais seguro você usar aquela chave pública. Por isso o certificado entra aí, nessa lista negra.

Então, por que é importante isso, né? O certificado tem um prazo de validade, se ainda não chegou no final dessa validade aquela informação deve ser considerada verdadeira. Mas, se foi comprometida a chave privada, você não pode mais usar aquela chave pública, né? A segurança da comunicação foi

comprometida, você tem que ter um jeito ali de revogar aquela informação. Então você coloca aquele certificado nessa lista.

E por que eu estou falando tudo isso, né? Se vocês repararem, eu falei, modelo de PKI, isso soa um pouquinho familiar, né? Então esse modelo aí é a base do que a gente tem hoje do RPKI. Então, o PKI do RPKI é a mesma sigla de Public Key Infraestruture. Só que aí, no caso, é Resource Public Key Infraestructure para o caso do RPKI.

Então vamos ver propriamente como funciona a segurança no RPKI. Então a estrutura do RPKI pode ser dividida ali, em duas partes, né? A gente tem uma primeira parte que é o caso ali de certificação de recursos. Então é a parte que você anuncia os prefixos no RPKI, e aí qualquer um que possui recursos de numeração pode aderir ao RPKI nessa parte. Já a segunda parte ali, da validação na origem, é a parte em que qualquer um pode fazer a consulta às informações disponíveis no RPKI para fazer as validações das rotas aprendidas ali no BGP.

Bem, então vamos falar primeiro aí, da parte de certificação de recursos. Essa parte aí vai funcionar naquele trecho ali em vermelho, da estrutura ali do RPKI. Então ele vai funcionar basicamente ali com as autoridades certificadoras e o repositório.

Então qual seria a ideia da certificação de recursos? Seria certificar os recursos alocados de IP e ASN. A ideia é usar ali uma cadeia de certificação, assim como eu mostrei antes. E a gente gerar certificados não apenas ali validando o dono da chave pública, mas também quais são os recursos de numeração de IP e ASN que eu quero vincular.

A distribuição, hoje, de endereços IP é feita de forma hierárquica. A gente tem a entidade da Iana, que faz a divisão ali, em nível mundial, para cinco entidades ali, de nível regional, para cinco RIRs. E aí, cada uma dessas entidades regionais faz a distribuição de endereços IP na sua região, ou ali para alguma outra entidade de nível nacional.

No nosso caso aqui do Brasil, a gente tem a entidade de nível nacional, que é o NIC.br, e a gente está ali abaixo da entidade que rege a nossa região, que é a do Lacnic, que cuida aqui da América Latina.

Então vendo ali que a distribuição de endereços IP já é feita seguindo uma ordem, uma certa hierarquia? Para a cadeia do RPKI foi utilizada essa mesma hierarquia. Então, na cadeia de certificação do RPKI cada RIR, cada entidade regional, pode ser uma fonte autoritativa daquela região. Então, eles têm o poder e informações para ser a entidade confiável que vai atestar quais foram os endereços IPs alocados para quais ASNs.

Então esses RIRs vão funcionar como autoridades certificadoras, vão funcionar como CAs, certificando ali quais IPs foram alocados para quais sistemas autônomos. E, também, atestando qual é a chave pública daquele sistema autônomo. Isso também vai ser importante para usar no sistema do RPKI.

Então, o RIR pode ser conhecido ali também como uma trust anchor, uma âncora de confiança ali do sistema da cadeia de certificação do sistema do RPKI. Eles agem como autoridades certificadoras raiz. Então eles são CAs raiz. É o início da cadeia de certificação, são as entidades que todos têm confiança, todos têm conhecimento dessas entidades.

E aí, a partir dessas entidades, é gerada a cadeia. Então, por exemplo, da nossa região tem o Lacnic. Aí o Lacnic gera um certificado digital para a gente do NIC.br, que a gente está abaixo deles nessa cadeia. E a

gente, do NIC.br, gera o certificado digital para um provedor aqui, por exemplo, da nossa região aqui do Brasil.

Seguindo ali nessa cadeia de certificação é similar ao que eu mostrei ali na estrutura de uma PKI, que vai um gerando certificado para o outro, até chegar na última entidade, na entidade final.

Então, no caso, na nossa região tem a entidade de nível nacional, o NIC.br. Mas tem regiões ali, no caso, por exemplo, do AFRINIC não tem nenhuma entidade de nível nacional. Então, o AFRINIC vai gerar ali o certificado direto para as entidades finais, para os sistemas autônomos da região deles.

Um detalhe importante dessa cadeia é que as CAs raízes são os RIRs. A Iana não é uma raiz, não é uma trust anchor. Ela não faz ali, ela não inicia a cadeia do RPKI.

As autoridades certificadoras raiz da estrutura do RPKI são os RIRs. Então, aí nessa cadeia de certificação do RPKI, as autoridades certificadoras vão ser as que vão ali atestar propriamente quem tem qual bloco ali de IP, quem tem qual ASN. Então vai atestar ali os recursos de numeração. E os certificados ali das entidades finais vão ser os utilizados para verificar as assinaturas contidas ali nos documentos que vão estar disponíveis para a consulta no repositório do RPKI. Então aí tem uma diferença, o CA vai validar os recursos de numeração e o certificado de entidade final é que vai verificar as assinaturas digitais.

No repositório do RPKI, quais são os documentos contidos nele e o que a gente vai consultar depois nesse banco de informações? A gente vai ter os certificados digitais, então a gente vai ter ali os certificados do tipo X509 com a extensão dos recursos de numeração. Então as informações de quem, qual a chave pública, qual a ASN, qual o IP. Isso tudo vai estar em documento assinado por uma autoridade certificadora, uma CA, no caso aqui o NIC, ou do Lacnic, ou do ASN que gerou ali esse documento. Vão ter também ali a lista de certificados revogados. Assim como eu falei que no PKI tinha ali uma lista negra de certificados que não eram mais para ser considerados, aqui no caso do RPKI também tem essa lista. Então certificados digitais que tiveram a segurança comprometida e foram revogados estão listados aí.

A gente vai ter um documento ali chamado de ROA, Route Origin Authorisation. Esse documento propriamente, essa informação aí, essa ROA, é a que vai ter a informação da lista de prefixos que estão sendo anunciados por uma AS. Esse é o principal documento que vai ser consultado para fazer depois a validação das rotas ali no nosso BGP. Então vai ter esse documento aí, que a gente vai falar mais um pouquinho sobre ele daqui a pouco.

E vai ter ali um outro documento chamado Manifest, o manifesto, que no caso ele é uma lista de todos os documentos assinados por um AS. Então tudo que um AS gerou ali, um AS gerou 10 ROAs, então ele assinou ali dez ROAs, vão estar listados ali nesse Manifest. Ah, ele gerou ali uma lista de certificado revogado, ele revogou ali um certificado, vai estar aí também listado nesse Manifest. Ele gerou um certificado digital novo, vai estar listado aí. Então, é como se fosse um sumário, um indicezinho de todos os documentos assinados por um AS.

E aí, como eu tinha mencionado, a gente vai consultar depois esses repositórios do RPKI para obter as informações que a gente vai usar, para validar as nossas rotas do BGP, colocando políticas de roteamento para melhorar a segurança na comunicação no BGP.

Bem, então vamos falar propriamente um pouquinho mais sobre as ROAs. Como eu tinha dito, a ROA é um documento que basicamente fala qual o prefixo pode ser anunciado, está sendo anunciado por qual AS.

Então você pode considerar aí, que é um documento que está falando mais ou menos essas palavras: "Eu autorizo o ASN XXX a originar esse prefixo aqui". E aí eu assino embaixo, né?

Então vamos ver aí quais são os elementos propriamente que estão dentro da ROA. A ROA tem um nome, então você pode colocar ali o identificador para aquela ROA. Tem lá o número do AS, o ASN que está sendo autorizado a fazer o anúncio do prefixo. Tem o prefixo em si. Ali no nosso exemplo aí, da direita, no slide, tem o prefixo IPv6, é o 2001:Db8::/32. Essa ROA em específico, ela permite ali o prefixo máximo e até um /48. Então esse ASN aí 65538 pode anunciar esse /32 ou qualquer outra coisa até um /48. E esse documento aí tem validade de um ano, e é assinado pela organização aí responsável por esse bloco de endereço IPv6.

Um detalhe importante aí é que a gente tem prefixo/32. E ali o prefixo máximo é até um /48. Se não for especificado nada ali no prefixo máximo, ali no lugar daquele /48, se não for colocado nada na geração da ROA, o único prefixo que vai poder ser anunciado por esse AS 65538 seria esse /32. Então, se você não especificar ali o intervalo de prefixo... do prefixo até um prefixo máximo, o único anúncio que isso pode ser feito é o que está explícito ali, anotado no prefixo. Então no caso seria um /32.

Como tem ali até um /48, pode ser anunciado qualquer coisa aí nesse intervalo. Não pode ser anunciado nada mais específico do que um /48. Isso também não pode. Então, aí, cuidado com esse detalhe.

Aí alguns detalhes sobre as ROAs, né? Todos os prefixos anunciados devem estar cadastrados em uma ROA. Então para ter a validação naqueles prefixos que você anunciou, você precisa gerar uma ROA para esses prefixos. Cada ROA contém apenas um ASN. Então, se você quer deixar... o seu AS está anunciando ali um determinado prefixo e você quer permitir que o AS ali de uma empresa parceira sua também anuncie aquele prefixo. O que você vai precisar fazer? Você vai precisar gerar uma ROA, tanto para o seu AS, quanto para o AS desse seu parceiro. Então um detalhe importante, como o bloco de endereços é seu, quem vai assinar aquela ROA é você, porque você é o detentor daqueles recursos.

Mas, dentro daquela ROA, não precisa necessariamente ser o seu número de ASN, você pode colocar ali o ASN de uma outra entidade. Então você pode gerar uma ROA ali para o seu prefixo, para o seu bloco de endereços atrelado ali a um outro AS. No caso aí, como eu disse, por exemplo, um parceiro seu que você quer permitir o uso, o anúncio ali daquele bloco de endereços.

Como eu disse, quem vai assinar propriamente a ROA vai ser o responsável, a organização que está com aqueles recursos de IP alocados para ela. Então, se os blocos de endereço são seus, então você vai assinar aquela ROA. Outra pessoa não pode fazer isso, né? Ela não tem ali o direito de assinar aquela ROA, porque isso não vai estar validado ali na cadeia de certificação. E é importante que essas informações das ROAs estejam publicadas ali e acessíveis nos repositórios que vão ser consultados depois, no RPKI.

Como eu tinha dito, se você quiser alocar ali um bloco de prefixos para uma outra entidade, para um outro AS, né? Você é detentor daqueles recursos de numeração, e você quer alocar para outra entidade fazer aquele anúncio. Você pode. O sistema do RPKI permite isso. E aí, como que você pode fazer isso, né? A primeira opção é você gerar a ROA, que nem eu falei. Você vai gerar aquela ROA, você vai assinar, e no lugar ali do ASN você vai colocar o ASN da entidade aí que você quer permitir que use aquele bloco de endereços. Outra opção seria você gerar um certificado digital de CA. Então de autoridade certificadora. Então, seria como se você fosse uma autoridade certificadora pai, e vai gerar ali um certificado digital para uma outra entidade que vai ser ali uma autoridade certificadora filha. Então você vai assinar ali um certificado digital alocando lá aquele bloco para essa outra entidade. Aí, no caso, essa entidade vai gerar a

ROA, com essa informação, e ela que vai assinar. Essa assinatura vai estar validada pelo certificado digital de CA que você gerou para ele. Então vai estar seguindo ali na cadeia. Então, no caso, Lacnic gerou certificado do NIC, o NIC gerou seu certificado digital, e você gerou o certificado digital para essa outra entidade. Então valida toda essa cadeia, então está validado ali, essa outra entidade pode fazer a geração daquela ROA.

Detalhes importantes aqui, né? Se existir uma ROA para um determinado prefixo, a origem da rota desse prefixo vai ser validada, com certeza. Existindo a rota para aquele prefixo, aquele prefixo vai ter a origem dele validada ali na cadeia do RPKI. Por isso, detalhe importante, publicar ROAs incorretas é pior do que não publicar ROAs nenhuma. Então, tomem cuidado.

O que a gente tem hoje na internet é a maioria ainda não está usando o RPKI, pelo menos aqui na nossa região do Brasil, então não tem nenhuma ROA publicada naqueles prefixos, mas a internet está funcionando para essas orientações que ainda não aderiram RPKI. Agora, se elas publicarem uma ROA incorreta, essa ROA pode acabar invalidando o anúncio daqueles no BGP. Então, tome cuidado!

Calma, eu não tô querendo botar medo em vocês. Eu só quero que vocês tomem aí, um pouquinho de atenção, porque isso é importante.

Aí no slide tem até um exemplo de uma organização de um AS aí, que eles estavam usando o RPKI. E aí eles tinham feito ali o anúncio de um /16. No RPKI, eles geraram uma ROA, estavam anunciando no BGP ali aquele /16 e tava tudo ok. Só que aí no caso, eles decidiram mudar o anúncio deles no BGP para /17. Então eles quebraram aquele /16 e anunciaram ali dois /17 na rede. E aí, no caso, a ROA gerada por essa entidade só comportava ali o /16. Não permitia o anúncio de /17s. Então o que aconteceu? Se pode anunciar/16, mas não pode anunciar /17, então aqueles anúncios /17 foram considerados incorretos dentro da estrutura do RPKI. Então aquelas rotas foram invalidadas. Por isso que a gente fala: Toma cuidado! Se você anunciar errado as ROAs, isso pode acabar afetando os seus anúncios no BGP. E isso também implica aí em mais uma atenção que a gente tem que tomar. Se você for fazer qualquer mudança nas suas políticas, ali nos seus anúncios do BGP, faz essa mesma mudança ali, atualiza suas informações no RPKI. Não esquece de atualizar a informação também nas ROAs.

Existem dois modos de operação no RPKI. Existe um modo hospedado, em que é adotado aí, por exemplo, no caso pelo Lacnic. E existe um modo delegado, que é o que foi adotado aqui inicialmente para o RPKI aqui da nossa região do Brasil, pelo NIC.br.

Então, qual é a diferença de cada um desses modos, né? O modo hospedado, que foi adotado inicialmente aí, para incentivar a adoção do RPKI, ele parece ser um pouquinho mais simples e amigável para o pessoal que está entrando nessa estrutura do RPKI. Então ele centraliza toda aquela estrutura de certificação de recursos nas entidades dos RIRs. Então o AS faz solicitação ali para o sistema do RIR para fazer qualquer ação no RPKI.

Seria seguindo mais ou menos aí esse esquema, que, no caso ali tem por exemplo AS 65536. Ele vai ali acessar o sistema da interface do RIR, e fazer ali a solicitação. "Ah, quero gerar um par de chaves". "Quero assinar ali um certificado digital". "Quero gerar uma ROA aqui para o meu prefixo". Isso tudo aí é feito a partir dessa interface aí do sistema do RIR. E toda aquela parte ali de geração de certificados, de geração de documentos assinados e publicação ali dos documentos, das ROAs, é tudo feito ali pelo RIR. É o RIR que vai ficar cuidando disso tudo.

Já o modo delegado, o que ele tem de diferente? Ele é um sistema mais distribuído, né? Então ele não está mais centralizado ali no caso no RIR, vai estar centralizado aqui no NIC.br. Então ele é um sistema mais distribuído de autoridade certificadora. Ele foi feito assim, seguindo propriamente a ideia de uma PKI, de uma infraestrutura de chaves públicas. Ele facilita a automatização por parte do sistema autônomo, que, então, não vai ter que ficar mais pedindo para o RIR gerar ali um documento assinado, uma ROA, por exemplo. Ele mesmo pode gerar a ROA. Então ele tem maior facilidade aí, em tomar essas ações. Ele vai ter aí um pouco mais de autonomia. O gerenciamento aí, como eu tinha dito das ROAs, agora, quem vai criar as ROAs e assinar, fazer esses documentos vai ser o detentor aqui dos recursos de numeração. Não vai ficar mais na mão de outra pessoa. No caso aí do RIR, do NIC não, vai ficar na mão de ninguém, nenhuma autoridade certificadora, nenhuma outra entidade. Você vai ter que cuidar de gerar suas próprias ROAs e atualizar as informações das suas ROAs.

O controle agora da chave privada fica na mão do sistema autônomo, do AS. Então agora você vai ter que tomar conta da sua chave privada. Ela é importante. Como eu disse, a segurança do sistema todo está em cima das chaves criptográficas. Então esse modelo delegado, cada entidade vai cuidar agora da sua chave. No modelo hospedado todas as chaves ficavam guardadas ali e centralizadas no RIR. Isso não é bom, pelo ponto de vista de segurança. O ideal é que só o dono daquela chave tenha essa informação. Então, não tem porque o RIR conhecer essa sua chave, então só você vai conhecer a sua chave e você vai ter que guardar ali ela de forma segura e protegida nesse nosso modelo delegado. E você também pode gerar certificados digitais para autoridades certificadoras filhas de você, como eu tinha mencionado antes ali. No caso das ROAs você pode gerar um certificado digital aí para um outro AS. Aí esse AS ali vai ganhar aquele bloco de endereços que você está alocando para ele. Ele vai poder gerar as ROAs dele em cima desses endereços que você alocou para ele. Então você vai ter mais essa autonomia e liberdade nesse sistema aqui, no modo delegado.

Para o funcionamento do modo delegado, para a comunicação entre essas diversas autoridades certificadoras, para atualizar as informações, pedir os documentos, enviar os documentos, os certificados digitais, as chaves públicas - não envie chaves privadas - toda essa comunicação é feita por esse protocolo, como é conhecido como protocolo UpDown. Ele vai fazer a geração e validação ali dos documentos que vai para os repositórios. Ele também vai cuidar de fazer comunicação para geração dos certificados assinados, da CA pai para CA filha. Ele também vai ajudar ali na atualização, e na publicação das suas ROAs, seja usando aí um repositório próprio, que você vai ter que ter alta disponibilidade aí nesse seu repositório, ou você pode usar um repositório de uma outra entidade, de um terceiro para fazer essas publicações dessa informação.

Por exemplo, o repositório do NIC. Então você pode armazenar as suas ROAs nos nossos repositórios, para ser consultado pelos outros sistemas. Então o envio aí dessa informação dessa ROA para nosso repositório também vai ser através desse protocolo aí UpDown.

Mas, se você quiser, também, manter essas ROAs publicadas em um repositório seu, não tem problema, você pode. Só é importante que você tenha esse repositório sempre acessível, com alta disponibilidade. Então é importante ter aí uma máquina que garanta que a informação dessas ROAs vai ser consultada nesse repositório. Então suas ROAs vão ser consultadas aí através desse repositório pelos outros sistemas autônomos.

Ok, como é que eu faço? O que eu preciso aí, para entrar no sistema do RPKI aqui, no caso da nossa região do Brasil, que segue aí esse modo delegado? Você precisa do software de uma autoridade certificadora. No

caso aqui o que o NIC.br adotou, que você pode adotar, é o software do Krill. Criado pela NLnet Labs. Mais para frente a gente vai explicar direitinho aí como é que você pode usar, como é que você usa esse software para fazer a geração dos seus certificados digitais, para publicação das suas ROAs. E, como você precisa de um servidor de publicação. Como eu mencionei, você pode ter um servidor próprio de alta disponibilidade ou usar aí, um outro servidor, por exemplo, do NIC.br.

Uma coisa importante, para você que está usando o RPKI aqui na nossa região do Brasil, que adotou aí o modo delegado, é de extrema importância que você mantenha o seu servidor Krill sempre de pé. Então, você vai usar ele para gerar o certificado digital, gerar suas ROAs. Mas aí, depois, você não pode desligar esse servidor: "Ah, gerei minhas ROAs. Publiquei elas, está tudo ok, estão publicadas, posso desligar esse servidor". Não, você não pode. Você tem que manter esse servidor sempre ativo. Por quê, né? Ele vai manter atualizações constantes e automáticas ali com o sistema do RPKI.

No caso, ele vai sempre atualizar ali as informações periodicamente, usando o protocolo UpDown, fechando ali uma comunicação com o nosso servidor Krill, aqui do NIC. Então é importante você manter ativo também, porque, todos os documentos dentro do sistema do RPKI têm um prazo de validade. Aí, a partir dessas atualizações constantes, que acontece pelo protocolo UpDown, ele vai validando. Ah, o quê? Aquele documento ainda tá válido, aquele documento você ainda está usando ele, e ele vai renovando periodicamente e automaticamente.

Se você desligar o seu servidor Krill, então ele não vai conseguir fazer essa renovação ali das validades dos documentos. Então seus documentos todos vão expirar. Então, tudo que estava sendo validado não vai ser mais validado, né? Os documentos não vão ser mais consultados, porque eles vão ter expirado ali o prazo de validade.

Isso é um problema? Sim e não, não é? Não é um problema tão grave. É um problema, porque as suas rotas não vão ser mais validadas no sistema do RPKI, mas elas também vão não vão ser invalidadas. No caso aí, as suas rotas vão virar desconhecidas, vai ser como se você não estivesse usando o RPKI. É isso que vai acontecer.

Então como uma forma de ajudar o pessoal da nossa região do Brasil que começou recentemente a adotar o RPKI nos seus sistemas, o sistema do Registro.Br, ele tem ali um monitoramento. Então se tiver tudo ok, você configurou ali o RPKI no sistema, está ok, vai aparecer ali: Ambiente RPKI ok. Se o seu servidor Krill, por exemplo, ficar inacessível, tiver algum problema, seu servidor foi desligado, depois de um tempo a comunicação ali do UpDown com o nosso servidor não vai acontecer. E aí o sistema ali do Registro.Br, ele mostra uma mensagenzinha, falando que tem ali algum problema, algum possível problema para você verificar.

Então, no momento, está tendo esse monitoramento para ajudar o pessoal a ficar aí atento. Pessoal aí, que está vendo como é que usa o RPKI e está aprendendo, ainda.

Então a parte de certificação de recursos era isso. A parte mais voltada ali, envolvendo a parte de segurança, de criptografia, de chaves criptográficas, de certificado digitais, com a cadeia ali de certificação.

O que é o ponto importante de você lembrar dessa parte é: Se você for adotar o RPKI... Na nossa região do Brasil, a gente usa o modo delegado. No modo delegado, o que você precisa, né? Você vai precisar ali gerar as suas chaves criptográficas, gerar ali suas informações de autoridade certificadora, comunicar essas informações junto com o sistema do Registro.br. E aí, depois, você vai fazer a publicação das suas ROAs, falando ali quais são os prefixos que você está usando no BGP. E aí essas ROAs devem ficar aí disponíveis

em repositórios do RPKI. Seja um repositório seu aí, de alta disponibilidade ou um repositório de terceiro, por exemplo, repositório do NIC.br, que a gente está fornecendo ali, disponibilizando para que seja feita a publicação dessas ROAs.

Agora eu vou passar para o Eduardo falar aí, sobre a parte de validação na origem.

**SR. EDUARDO BARASAL MORALES**: Bom, agora que a gente já viu a parte de publicação dos ROAs, agora a gente vai ver a segunda parte, que é a validação na origem.

Só que, lembrem, isso daqui é só uma lapidação de um conteúdo bem extenso. A gente não vai falar tudo, não vai dar tempo. A gente tem muitas coisas ainda para falar. A gente quer fazer ainda até uma parte prática com vocês, para vocês conseguirem publicar os seus ROAs.

Essa segunda parte, então, é só mais um complemento. Se vocês querem saber um pouquinho mais, dá uma olhada lá no vídeo que a gente gravou na semana de infraestrutura.

Então, lembrando ali a estrutura do RPKI. A gente já viu sobre a autoridade certificadora. A gente viu sobre os repositórios. Agora a gente vai ver a parte do validador junto com o roteador. E, através disso, a gente vai conseguir demarcar as rotas, se elas estão válidas, inválidas ou desconhecidas, e depois tomar uma decisão no nosso roteador para saber se a gente vai aceitar aquelas rotas, ou vai descartar aquelas rotas, ou tomar alguma outra atitude relacionada às políticas do BGP.

Então, vamos dar uma olhada. A questão ali da validação da origem trabalha com dois componentes básicos, o validador e o roteador. O validador é um outro software, que você vai instalar lá no servidor, em uma máquina virtual, seja onde for, que vai trabalhar com a validação dos objetos certificados. E nesse software ele vai trabalhar indo em toda aquela cadeia de certificação, descobrindo se a informação está correta, e, depois, condensando as informações junto lá com o que foi enviado dos caches, para passar para o roteador tomar a decisão sobre as rotas. Então ele vai meio que fazer um resumo de todas aqueles ROAs que ele vai pegar lá, de todas aquelas entidades certificadoras, e vai passar para o roteador.

E aí o roteador vai fazer validação das rotas. Ele já trabalha com o BGP, ele vai ver: "Oh, essa rota, ela está assinada? Ela é uma rota válida? Ela é uma rota inválida?". E depois vai tomar decisão sobre o que for melhor ali para o sistema autônomo, o que o administrador de redes tomar como melhor decisão de tráfego. Então, ele obtém as informações do validador e aí ele vai conseguir influenciar no roteamento.

Então, dando uma olhada ali como que funciona todo esse fluxo. Então, olhando ali, a gente tem o ROA, com prefixo 2001 db8/32 do ASN 65538, e o prefixo máximo até um /48. Então do 32 até o /48 o AS 65538 pode criar ali uma rota de tamanho 33, de tamanho 34, 35 e assim por diante, e mandar que você deve aceitar. Porque vai estar validado.

Então dá uma olhada ali nas rotas que a gente está recebendo no nosso AS 65536. A gente está recebendo a rota /32 vindo do 38 de origem, e o /48 vindo do 40 de origem.

E quem tem a informação válida? É o 38, como a gente já viu. Ele é o dono 2001 db8/32. E ele que assinou ali o ROA. Então, com essa informação, você vai dizer que aquela rota vindo de origem 38 é válida; e a vindo de origem 40 inválida. E aí você pode tomar a decisão de descartar a rota inválida e ficar só com a rota válida. E o seu tráfego vai fluir para o destino correto. Perceba que a gente já está começando a evitar ali um roubo de prefixo, um vazamento de rotas que não deveria ter chegado até você.

Então falando agora um pouco do validador. O validador, ele faz a conexão com repositórios confiáveis, que é a do Ripe, do Lacnic, os RIRs que a Erina já comentou. E ele vai falar com esses RIRs, nesses repositórios, através de um protocolo, geralmente o Rsync ou o RRDP.

Conversando com esses repositórios, ele vai baixar as informações dos ROAs, vai guardar em um Cache e vai fazer atualizações periódicas. E ele vai pegar aquela informação e vai validar. Ele vai verificar as assinaturas dos ROAs e percorrer todo aquele caminho de certificação. Vendo que está tudo ok, ele vai fazer o quê? Um resumo que vai guardar aí no VRP. Ele vai passar esse VRP para o roteador, através de um protocolo chamado RPKI-to-Router, e com essa informação transmitida para o roteador, o roteador vai conseguir tomar decisão sobre aquela rota, se ela é válida ou não.

Então, no validador, como a gente já disse, ele tem que estar em um software à parte, em uma máquina à parte. E existem vários softwares disponíveis para isso. A gente tem Routinator, que a gente vai mostrar ali no laboratório, junto com o Tiago, como utilizar. Tem o do Dragon Research Toolkit, esse daí já é um pouco mais antigo, a gente recomenda não utilizar, ele não está ai tão up to date, ele não está tão atualizado. Mas tem outros muito bons, como também o RIPE Validator. Temos ali também o OctoRPKI, da Cloudflare. E temos ali o Fort Validador que foi criado pelo NIC México junto com o Lacnic, esse daí também é uma recomendação para vocês instalarem.

E outra, a gente recomenda que se utilize mais de um validador distinto. Então, você não deve ter só uma máquina, você deve ter duas máquinas para ter ali uma redundância. Então instala ali o Routinator e instala o Fort, ou o Ripe Validator, escolhe um outro ali do seu gosto, faz ali um conjuntinho de dois. Mas não escolham o mesmo, não pode ser dois Routinators, dois Forts. Por quê? Se um tem problema, um bug, vai prejudicar o funcionamento do seu provedor, do seu sistema autônomo, porque o bug vai estar nos dois. Então quando você tem redundância de outro vendo, isso vai melhorar muito para você. Porque se algum tiver problema, o outro está te mantendo em pé com todas as informações corretas. Então, por isso, trabalhem com os dois.

Do roteador, lembra? O roteador, ele precisa conversar com o validador. Então você precisa ver se o seu roteador tem suporte. Aqui eu vou mostrar alguns que já possuem suporte já há algum tempo, mas existem outros que não têm esse suporte, essa validação de origem, o RPKI para poder conversar com o validador e depois tomar uma decisão.

Nesse caso, ou você vai ter que trocar o roteador, ou esperar ali uma nova versão daquele vendor(F), daquele roteador, ou, então, no mínimo, pedir para seu upstream, o seu provedor de trânsito fazer a validação por você. Se ele te mandar as rotas todas limpinhas, todas bonitinhas, isso daí já vai te ajudar bastante. Por quê? Porque ele já vai te passar rotas corretas. Então você não vai receber informação errada. Mas é claro, é bom que todo mundo faça! Não dá para deixar ali nas costas dos outros.

Então, aí, mostrando alguns roteadores. Juniper, Cisco, Nokia, temos o Bird, o OpenBGPD. Temos ali o GoBGP, VyOS. Existem ali vários softwares que você pode trabalhar com o RPKI no roteador. Então, fiquem atentos aí, vejam se vocês têm alguns desses roteadores e já comecem a implementar também a questão de validação.

Então, os roteadores, eles recebem os VRPs, que é aquele resuminho, e eles vão utilizar isso para tomar uma decisão de roteamento. Então ele recebe aquelas informações dos ROAs lá, todas resumidas, e, quando ele recebe a rota, ele vai conseguir fazer uma demarcação na rota, se ela é válida, inválida ou desconhecida. E depois ele vai tomar uma atitude em cima dessa demarcação, como, por exemplo,

descartar as inválidas, ou descartar as desconhecidas, ou, então, mudar só a community, ou local preference, dá para fazer um monte de coisas.

Mas como que uma rota é considerada válida? A origem e o prefixo máximo estão de acordo com a informação do ROA. Inválida, a informação não está de acordo com o ROA. E desconhecido, não existe ROA para o prefixo verificado. Então são esses três estados.

Vamos dar uma olhada ali com alguns exemplos. Então a gente tem ali um ROA 65536, prefixo 10/16, com comprimido máximo até o /18. Vamos olhar cada um dos exemplos. Olha, recebi rota 10/16 com 65536 de origem. Tá certo? Opa, tá dentro do ROA. Então tá certo. Recebi ali o 10.0.128.0/17, AS de origem 65536. Tá certo? Opa, tá certo. Está dentro do ROA, eu aceito e já marco como válida.

Vamos ver outro caso. Recebi o 10/24 do 36, do sistema autônomo 36. Tá certo? Ah, está extrapolando. Afinal, o ROA está marcando ali do 16 ao 18. Esse é o 24. Então não está certo. Isso daí está um prefixo além do que você permitiu. Então é uma rota inválida.

Vamos ver outro exemplo. 65540 mandando 10/18. Ou seja, prefixo está dentro, mas o AS de origem não está certo. Então está errado. É uma rota inválida.

Outros casos, desconhecido, né? 10/8 vindo do 36. Opa, agora a gente está falando de um prefixo menor do que tem no ROA. Então eu não consigo dizer se existe aquela informação. Então, desconhecida.

Depois disso, o 10/8 do 65540. Também não condiz com aquele ROA. Então não sei, é desconhecido. O ASN está diferente, o prefixo está diferente, ele é um prefixo menor, no caso é menor na questão do 10/8, e a gente não consegue tomar nenhuma decisão sobre isso. Então ela é desconhecida

Então, aqui, a gente vai falar um pouquinho sobre as políticas de roteamento que podem ser estabelecidas em cima da validação das rotas. Você pode ali mudar o local preference, mudar as communities e colocar filtros. Mas qual que é a recomendação? Bom, a primeira vez que você faz isso não vamos destacar todas rotas. Afinal, você não tem uma segurança sobre o que está acontecendo. Então vamos demarcar elas. Marca com communities, communities das válidas, communities das inválidas e as communities das desconhecidas. Depois que você olhar sua tabela de roteamento com todas as demarcações de communities, você vai conseguir enxergar qual vai ser o impacto no seu provedor.

Não tem ali grandes impactos. Na verdade, as inválidas são realmente rotas lixo, alguém fazendo coisa errada. Vamos descartar rotas inválidas. E, mais para frente, quem sabe, a gente consiga até descartar as desconhecidas.

Hoje em dia não dá para pensar em descartar as desconhecidas, porque, na verdade, muita gente ainda não usa o RPKI. Mas, quando todo mundo utilizar, a gente só vai ter rotas todas validadas. Então, aquelas desconhecidas são rotas extras, rotas que não deveriam estar lá, e a gente vai poder descartar.

Então, para agora, marca com community e depois vamos descartar as inválidas. Aquela desconhecida, se você quer trabalhar com alguma coisa, diminui o local preference dela, diminui um pouco a preferência dela, deixa ela ir como rota um pouco pior, e aí, você vai ter ali alguma atitude. E, depois, você pode pensar, no futuro, um dia, descartar as desconhecidas. Mas, por hora não. Vou mostrar para vocês os gráficos de utilização de RPKI, ainda não está nesse estágio para a gente pensar nas desconhecidas nesse requisito de descarte.

Então, como estamos? Vamos dar uma olhadinha aí. Então aqui já mostra o gráfico de adoção do RPKI pelo mundo. Você pôde ver que aqui no Brasil a gente ainda está com uma adoção um pouquinho baixa. O verdinho está bem clarinho. Mas isso é porque a gente está construindo essa base a partir de agora. Foi ali lançado em 2019, e aí pessoal começou a utilizar RPKI agora. Antes, não tinha a possibilidade de você trabalhar com RPKI aqui no Brasil. Diferente ali, dos outros países do mundo, que muitos já tinham algum suporte ali do seu RIR para trabalhar com RPKI. Então vocês vão ver ali algumas regiões muito mais avançadas, tá? E outras ali muito menos avançadas.

Então, aqui no Brasil, agora a gente precisa criar essa cultura de trabalhar com o RPKI, de adotar o RPKI.

Então, por enquanto, aqui no Brasil, está um pouquinho devagar. Mas vocês podem ver que os outros países da América Latina estão trabalhando bem. Então vamos continuar fazendo essa questão do RPKI e vamos transformar o Brasil em um orgulho na adoção do RPKI.

Então, ali, vamos fazer também uma análise da tabela completa do BGP. Isso também é legal de a gente ver dos anúncios de RPKI. Lembra que eu comentei que das desconhecidas não dá para a gente descartar? Olha, são 80% de todas as rotas que você recebe. Se você descartar 80% das rotas, você está descartando quase as rotas do mundo todo. Então não dá para a gente pensar nisso agora.

Agora, Rotas inválidas. São ali, 5 mil rotas, 6 mil rotas, são rotas que estão erradas. Se a gente descartar elas, a gente já fica com roteamento muito melhor, mais conciso. E as rotas válidas, a gente tem ali perto de umas 200 mil rotas. Quase ali 20% de todas as rotas enviadas. À medida que a gente for utilizando, e cada vez mais tiver provedores utilizando, aqui em verdinho tende a aumentar, e o amarelinho tende a diminuir. E, por favor, espero que o vermelhinho também diminua, tendendo a zero, que ninguém mais erre na questão ali de rotas inválidas.

Um outro gráfico que a gente mostra ali, os sistemas autônomos que tem mais prefixos validados por RPKI. No caso aí, a gente não está vendo nenhum brasileiro nessa primeira listagem, mas quem sabe, no futuro, a gente não acaba encontrando um brasileiro aí? Vamos torcer para tudo dar certo.

Agora vamos botar a mão na massa. Passar a voz para o Tiago, que vai explicar para vocês como implementar o RPKI. No caso ele vai trabalhar com o Krill, nós vamos utilizar a parte de publicação, vamos fazer uma entidade certificadora, autoridade certificadora, e vamos conversar com o Registro.Br para depois publicar os nossos ROAs. É aquela primeira parte. Essa segunda parte a gente vai ter que deixar para um tutorial futuro. Ou então você dá uma olhadinha lá na semana de infraestrutura que a gente já gravou no final do ano passado. Tá? Então eu vou passar a vez agora para o Tiago. Tiago, manda bala.

**SR. TIAGO JUN NAKAMURA**: Então, pessoal, sejam muito bem-vindos ao tutorial sobre RPKI.

Meu nome é Tiago Jun Nakamura, e eu vou estar fazendo aqui, agora, com vocês, a experiência de como que a gente configura o Krill do lado do provedor.

Então, como a gente viu na parte anterior, existem duas etapas importantes para o RPKI funcionar.

Então tem a parte de instituição que vai validar as informações para vocês, e tem a parte nossa que precisa enviar o que a gente quer que seja validado no RPKI.

Então, a instituição que vai fazer a validação é o Registro.Br. A instituição que vai divulgar as ROAs, com as informações referentes ao nosso AS somos nós mesmos, né? Então a gente precisa fazer essa configuração do nosso lado.

Então como que eu posso fazer isso? Tem diversas formas, o ideal é ter uma máquina dedicada para isso. Pode ser uma máquina virtual. No nosso caso aqui, a gente está fazendo com um Linux Mint, mas poderia ser qualquer máquina que suporte o Krill. Para verificar se eu consigo rodar Krill na minha máquina ou não, recomendo acessar esse site aqui, Read The Docs, do RPKI. Então esse site aqui ele é tipo um Wiki, com todas as informações necessárias para fazer a configuração aqui do Krill. Então ele explica quais são os requisitos, como é que eu instalo, como é que eu rodo tudo direitinho.

Então, essa máquina está zerada, vamos fazer a instalação aqui do zero. Então eu vou no install and run, e aí eu sigo o passo a passo aqui que ele está indicando no site.

Então ele fala: Se você usa uma máquina baseada em Ubuntu, você pode instalar aqui no próprio pacote Do apt-get. Então ele fala aqui... Coloca essa linha aqui no etc/apt/sources.list. Então como é que a gente faz isso. Opa. A gente vem aqui. Vou entrar como administrador.

E aí ele fala para entrar aqui no sources.list ou sources.list.d, depende do seu sistema operacional. Vamos ver aqui qual que é o nosso. APT, no nosso é o sources.list.d.

Aí ele fala para inserir essa linha referente aqui ao pacote deles. Então a gente vai abrir aqui o arquivo. Então pega aqui.

A gente pode inserir aqui no final. Pode criar um arquivo novo, se você preferir, porque esse aqui é o arquivo do repositório oficial, mas não faz diferença. É bom ver qual é a nossa distro, é o focal, então é esse aqui. Então a gente dá um ctrl+c, ctrl+v, beleza.

A gente salva as configurações. Depois ele pede para adicionar a chave, né? Senão ele vai reclamar que ele não reconhece esse repositório. Então a gente insere aqui a chave do repositório para ele aceitar no apt-get. E ele manda dar um update. Então a gente dá um apt-get update.

E ai ele fala para instalar aqui o Krill. Então a gente dá apt-get install Krill. Ele vai instalar. Então, pronto, seu Krill está instalado na sua máquina agora.

Aí ele fala para conferir aqui, né? É o /etc, /krill.conf. Então vamos lá, né? Vamos voltar aqui, /etc, aí deve ter um arquivo aqui chamado krill.conf. Então vamos dar uma olhada.

Esse arquivo, ele tem todas as informações que eu preciso configurar aqui para o Krill funcionar. A maioria delas já tem a configuração padrão aqui, que vai ser adequada para você. Então se você precisa fazer alguma configuração aqui, a maioria delas você não precisa mexer.

Então, para esse tutorial aqui, a única informação que você precisa, de fato, é configurar, ou sei lá, é ter certeza que você precisa saber é esse auth_token. Tá aqui, é basicamente a sua senha que você vai usar para acessar o seu Krill.

Então, no caso aqui, a gente vai colocar uma senha simples, mas lembra de colocar uma senha que você precisa colocar. Só para a gente poder lembrar aqui depois. Então coloquei aqui a senha Ceptro. E agora eu vou inicializar aqui o Krill. Ok.

Então vamos ver se está funcionando. Eu vou dar um ps aux pipe grep krill. Então aqui dá para ver o processo do Krill rodando. Então com a configuração /etc krill.conf. então a configuração está feita, o Krill está instalado e já está rodando aqui no nosso servidor.

Uma coisa importante, se vocês repararem aqui, eu estou no VirtualBox Se vocês forem fazer na máquina de vocês, é importante que essas máquinas permaneçam ligadas, tá? Por quê? Porque para o Krill validar as informações, ele vai conferir de tempos em tempos se você está de pé. Se você não estiver com a máquina ligada, quando o registro for fazer validação, ele vai ver que você está desligado. E, se ficar muito tempo desligado as suas ROAs que você publicar aqui, elas vão deixar de ser válidas. Então elas vão expirar porque ele não vai renovar a informação referente ao seu servidor Krill.

Então é importante que você configure esse servidor numa máquina que vá ficar, de preferência, sempre liga, tá? Não precisa ser um servidor dedicado, pode ser uma máquina virtual, pode ser container, pode ser a forma como você preferir.

Só tem que lembrar que ela não pode ser desligada. Então, se ficar um tempinho desligado, travou a máquina, precisei reiniciar para atualizar, não tem problema. Eu só não posso: "Ah, vou fazer só nesse laboratório aqui junto com tutorial e depois eu esqueço e desligo, nunca mais eu ligo ela". Então não vai funcionar, tá? Então essa é uma parte superimportante. Mas a parte de instalação do servidor Krill basicamente é essa. Ok?

Beleza. Então agora a gente já tem o Krill rodando, o que a gente precisa fazer? A gente precisa informar ao Registro.Br que a gente tem um servidor Krill e parear com o servidor Krill do Registro.Br. Então como é que a gente faz isso? Eu tenho que acessar o site do Registro.Br. E aqui eu posso ver aqui no 'acessar conta' no próprio site do registro, e entrar com o meu login. Uma coisa importante: Só o administrador do AS que vai ter acesso às configurações de RPKI aqui no sistema do registro.

Então, assim, o servidor pode ser qualquer pessoa que vai instalar, mas para fazer essa configuração Registro.Br servidor Krill precisa ser o administrador, o dono aqui do AS. Então, mesmo que você seja o contato técnico, não dá para fazer. Então toma muito cuidado na hora que você for fazer aqui. Lembra que só o administrador vai ter acesso à essas informações.

Então aqui tem um Captcha para ver se eu sou robô ou não. Vamos ver se eu sou ou não robô. Isso aqui é um ônibus? Isso aqui não sei, não parece, mas eu vou marcar. Esse é um ônibus. Ah-ha, não sou um robô. Então, acessei aqui o site do Registro, fiz o login. Vamos ver aqui as informações referentes ao AS dessa conta. E aqui, em titularidade, eu consigo ver aqui... Aqui a gente está no beta. Então é esse AS que está alocado aqui para essa conta.

Então, na hora que eu clicar aqui, ele vai me mandar para os dados do titular, e lá embaixo vai ter a configuração de RPKI. Então isso aqui só vai aparecer se você for o dono desse AS. Se você não for o dono, não vai dar para fazer essa configuração.

Então a gente entra aqui no configurar RPKI. Aqui, no caso, a gente já tem um RPKI funcionando. Fala assim: "E aí, né? E se eu mudar de máquina? E se eu precisar trocar o servidor, como é que eu faço?". Eu vou aqui e clico em desabilitar. Cliquei em desabilitar, pronto. É essa página que eu vou ver se eu nunca tiver configurado o RPKI na minha vida. Então eu vou entrar no site do Registro, não tenho RPKI configurado. Na hora que eu acessar, fizer login, clicar lá na configuração de RPKI, é essa página aqui que eu vou ter.

Então, habilitar o RPKI. Aí ele fala, né? Tem todo um passo a passo, aqui, algumas instruções se você tiver dúvida. Mas o que a gente precisa fazer? Ele está pedindo o child request. Para fazer esse child request a gente tem que entrar lá no Krill. O Krill, nessa versão mais nova, ele tem uma interface Web. E isso facilita muito a configuração aqui do que a gente precisa fazer. Para acessar o Krill, é o local host na porta 3000.

Não sei se ele vai forçar o HTPPS, na dúvida eu vou forçar aqui. Ele vai falar: "Cuidado. Esse certificado não é válido". E não é válido mesmo, porque é um certificado autoassinado. Então nesse caso eu sei que isso aqui está certo porque eu instalei o Krill nessa porta. A porta padrão nele é 3000 no local host. Então aqui eu vou ter que aceitar aqui, e aceitar o risco e continuar.

Beleza. Aqui é a interface do Krill. E aqui uma coisa interessante, eu posso ter aqui em português, as configurações do Krill. Então se eu não souber inglês, eu consigo fazer aqui tudo em português. Isso ajuda bastante, principalmente aqui no Brasil, né? Que nem todo mundo sabe e entende inglês, né? Então essa parte de eles terem traduzido para o português é bem legal.

Aí ele está pedindo aqui uma senha, né? Que senha é essa? Essa senha é a senha que a gente configurou lá no arquivo do krill.conf. Que é Ceptro. Então a gente coloca aqui a senha Ceptro. Aí ele pergunta aqui... Vamos salvar.

Aí ele fala: "Bem-vindo ao Krill. Eu quero criar aqui uma CA para você". Então essa CA aqui, basicamente é o nome que você vai dar para o seu certificado do Krill.

No caso aqui, a gente não tem nenhum critério, eu vou criar uma CA_Ceptro. Mas você cria com seu nome, e ela é basicamente um identificador do seu AS. A interface Web, ela está limitada para uma única CA. então, se você usar o Krill na linha de comando, você consegue criar múltiplas CAs. Aqui na interface web só dá para criar uma, que é a situação da maioria das pessoas. Então eu sou um provedor, e eu tenho só um AS, e eu faço essa configuração. Se eu tiver mais de um AS, aí, provavelmente, eu vou ter que usar a linha de comando para criar múltiplas CAs aqui, e identificar várias delas separadamente.

Então nesse caso aqui, na interface Web só vai dar para gerar uma. Então, eu vou aqui, crio a minha CA Ceptro. Aí ele vai avisar: "Não pode ser alterado uma vez que você criar". Ok.

Beleza. Criei lá minha CA, meu certificado. Aí lembra que estava pedindo o que aqui no registro? Chamado child request. Onde está esse child request? Ele está aqui no CAs pai. Então, na hora que eu colocar aqui no CAs pai ele tem aqui, requisição da CA filha. Então esse é o child request. É esse XML aqui, e eu preciso copiar e colar, né? Eu posso baixar ele em arquivo, mas, nesse caso aqui como eu estou em interface Web, eu vou fazer tudo direto aqui, eu dou ctrl+c, copio esse child request, e coloco aqui na página do registro. Então, ctrl+v. Coloquei aqui todo o XML do child request. Aí eu clico em 'habilitar RPKI'.

Beleza, né? Então o que aconteceu? O registro está verificando, viu que existe esse Krill, e começou já a parear e trocar informações através do protocolo UpDown. Então, a partir de agora, o seu Krill está já sincronizado com o Krill do Registro.Br.

Se eu quiser eu já posso começar a publicar lá as minhas ROAs, né? E as pessoas vão consultar o meu servidor Krill para verificar e validar essas ROAs. Se eu não quiser esse tipo de publicação, eu posso escolher deixar isso no registro. Tá? Para fazer isso eu preciso habilitar aqui a publicação remota. Tudo bem?

Se eu olhar aqui embaixo, ele está esperando uma resposta dessa CA pai. Então, se você olhar aqui, nesse XML, vocês vão ver que não é o XML que eu coloquei, não é o child request. Esse aqui é o parent response. Então, eu preciso fazer o quê? Eu preciso copiar esse parent response, então, ele inteiro, e colar aqui no meu Krill. Então eu vou copiar isso aqui e confirmar. Então, beleza, né? Agora o Registro.Br conhece o meu Krill e eu conheço o Krill do Registro.Br. Então agora a gente tem os dois lados configurados corretamente.

Ok. Aí agora o que falta fazer? A gente quer aqui, no caso, para esse tutorial, habilitar a publicação remota. Que é o quê? É basicamente dizer que eu quero que o Registro.Br armazene as minhas ROAs. Porque eu não quero que todo mundo que queira consultar as minhas informações precisem acessar o meu servidor Krill. Basta que eles acessem o servidor Krill do Registro.Br. Então uma forma de fazer isso é habilitando aqui a publicação remota.

Então eu vou clicar aqui na publicação remota, e ele vai pedir um publisher request. O que é o publisher request? É essa informação que está aqui em repositório. Então aqui eu tenho o XML do publisher request. Então eu vou copiar esse XML, e eu vou colar aqui no site do Registro. Eu vou clicar aqui em habilitar. Parece que foi ok. Uma coisa a se notar, este XML aqui não é o publisher request. Ele mudou aqui, virou o repository response. O que é isso? É a informação que eu preciso colocar aqui no Krill de resposta do repositório. Então eu vou copiar o repository response e colar aqui no meu Krill. Clico em confirmar pronto.

Então, basicamente, agora a gente já está com Krill pareado e eu estou com a publicação remota habilitada. Então todas as ROAs que eu gerar aqui, isso vai ser enviado para o Registro.Br, e ele vai armazenar essas ROAs para mim. Lembrando que, mesmo na publicação remota, eu preciso continuar com esse servidor Krill ligado, tá? Porque se eu estiver com publicações no Registro, mas o meu Krill estiver desligado, ele não vai conseguir validar essa ROA. Ele vai falar: "Mas de quem é a ROA? Ah, é do servidor Krill tal". Só que esse servidor Krill não está acessível. Então ele vai invalidar aquelas ROAs mesmo que você... mesmo que ela esteja com a validade ainda correta. Então, se ela vencer em 2025, mas ela não conseguir verificar de onde que está vindo a ROA, ele invalida mesmo assim. Então não é só data de expiração que o RPKI usa para validar aqueles certificados.

Então esse servidor Krill, ele é superimportante que ele esteja aqui ligado. Ok?

Então só para a gente lembrar como é que a gente fez configuração aqui. Fez login aqui no Krill. Colocou a senha lá que eu configurarei no krill.conf. Aí eu tenho que ir em CA pai, pegar aqui o child request, colocar no site do Registro. Eu vou receber aqui o parent response. Então eu coloco lá o child request, recebo o parent response.

Depois eu vou aqui em repositório, habilito a publicação remota, e recebo aqui o repository response. Tá? Então eu coloco aqui o repositório, ele já configura e autoriza lá o Registro a armazenar as minhas ROAs.

Então, a configuração basicamente aqui está pronta. O que falta fazer? Configurar as ROAs. Então agora sim, a gente vai configurar aqui o que eu quero anunciar para o RPKI. E acho que essa é a parte mais complicada, no fundo, que é o que eu quero publicado dentro da ROA? Se eu... O ideal é que as publicações das minhas ROAs sejam iguais às publicações que eu faço no meu BGP. Então, se eu anuncio, por exemplo, um /22 e um /24, eu deveria ter uma ROA desse /22 e desse /24.

Como é que eu sei o que eu estou publicando? Eu posso olhar nas configurações de meu roteador de borda, eu posso olhar no Looking Glass. O Krill, ele tem um recurso interessante aqui, que consegue verificar, através do Looking Glass do Ripe, o que está chegando lá referente ao seu AS. Então, na hora que você configurou aqui o CA pai com o Registro.Br, ele já pegou as informações referentes ao seu AS e já verificou o que tem na tabela BGP referente a esse AS.

Então, nesse exemplo aqui, ele viu que tem quatro anúncios aqui na internet. Então tem um /40 e um /48 em IPv6, e um /22 e um /24 de IPv4, dentro da internet. Nenhuma dessas informações, aqui, por

enquanto, estão sendo validadas por nenhuma ROA, porque eu não gerei nada. Então é uma tabela BGP normal mesmo, simplesmente está filtrando as informações referentes ao meu AS.

Se eu quiser configurar agora as ROAs, o que eu posso fazer? Bom, se eu quiser que as configurações sejam exatamente iguais a minha tabela BGP, eu simplesmente vou clicar aqui no 'maiszinho' e confirmar. O que ele vai fazer? Ele vai publicar uma ROA equivalente àquele anúncio que eu estou gerando.

Só que lembra que se eu fizer isso, toda vez que eu mudar o anúncio na tabela BGP, eu vou precisar mudar o anúncio aqui no RPKI. Então não se esqueçam que agora você sempre vai ter que checar duas vezes, tá? Então o seu anúncio BGP e as informações de RPKI.

Se eu não quiser ter esse problema de errar sem querer o anúncio da ROA, eu posso colocar aqui um intervalo de validade. Então, se eu clicar aqui de novo, vocês vão ver que aparece o meu AS, que eu posso mudar, porque se eu, por exemplo, se eu for um cliente de alguém e esse outro alguém que anuncia esse prefixo para mim no meu lugar, eu preciso colocar o AS dele aqui. Então pode mudar o número de AS. O prefixo, tá? Eu não consigo gerar uma ROA que não é referente a um prefixo meu. Então se eu quiser mudar aqui para, sei lá, né? É 2000... 2000 ainda sou eu, né? Vamos mudar aqui para 2182. Olha só o que ele vai falar: Ele não pertence a nenhum dos meus certificados atuais. Então eu não consigo gerar uma ROA que não é referente aos meus dados. Então assim, eu posso gerar ROA com outro número de AS, porque existe esse caso de eu ser cliente de alguém ou coisa do tipo, e a pessoa ter que divulgar os meus blocos por alguma razão, mas a questão do prefixo em si, eu só posso configurar ROAs referentes aos meus prefixos, tá? Então eu não consigo configurar ROA de outros prefixos. Então que isso aqui já é validado pelo próprio Krill.

Então, beleza, eu não vou conseguir gerar aqui coisas erradas, então eu vou configurar aqui, esse anúncio, essa rota IPv6. E tem aqui o comprimento máximo. O que é isso, né? É que intervalo que eu quero validar esse anúncio aqui de ROA. Então, por exemplo, eu poderia gerar uma ROA que fala: "Olha qualquer coisa que vai do /40 até o /48 é válido".

Na hora que eu gerar essa ROA, o que vai acontecer? Ele já vai verificar, inclusive ele vai falar: "Está abrangendo esses dois anúncios aqui, tanto o /40 como esse /48".

Então, se eu tenho essa insegurança de que talvez eu mudo muito os meus anúncios da internet e eu quero TER um pouco mais de segurança, eu posso publicar essa única ROA, que vai já abranger todos os meus anúncios. E eu posso fazer a mesma coisa para IPv4. Então eu vou pegar aqui esse /22, por exemplo. Então eu coloco aqui o 168181 200/22, e eu posso colocar aqui até o /24, que é o prefixo mais específico que eu posso anunciar na internet. Então, fazendo isso, todos os meus anúncios aqui já são validados.

Então o que essa ROA vai garantir? Qualquer coisa que venha na internet com esse anúncio aqui do /22 até o /24, com esse AS, é válido. Qualquer coisa diferente disso, não.

Então, se alguém anunciar uma coisa mais específica, um /25. Tudo bem, já vai ser filtrado pelo provedor. Mas suponha que chegue em algum momento isso em algum lugar, por essa ROA esse anúncio vai ser invalidado. Ou alguém tenta sequestrar o meu bloco e anuncia lá esse meu /24 na internet, ou um outro /24 meu. Ele vai verificar que o AS dele não é esse AS aqui, e também vai ser considerado inválido. Então essas duas situações, o RPKI, ele consegue invalidar Esses anúncios errados.

Agora, se alguém na internet divulgar um /24 e se passar pelo meu AS, então ele fala assim: "Eu sou AS 61580, e eu estou anunciado anunciando esse /24", para fins do RPKI isso vai ser válido. Por quê? Porque o anúncio está válido e o AS está válido.

Então esse tipo de situação, o RPKI não protege. Então se alguém se passar totalmente por você, falar que é o mesmo AS, é o mesmo anúncio, aí o RPKI não consegue distinguir você do cara que está fazendo essa configuração.

Então, assim, o RPKI, ele resolve grande parte dos problemas de erro de configuração. Então alguém vazou rota, alguém, sem querer, anunciou coisa mais específica e, sei lá, configurou errado lá o IP dele, e sem querer colocou o seu no lugar, isso ele evita. Agora, alguém que entende isso, consegue contornar fazendo, por exemplo, isso, coloca o anúncio mais específico, coloca sendo o seu AS, e o que deveria acontecer é que o upstream dele não deveria deixar isso passar. Então, se o upstream dele não filtrar isso, aí o RPKI não consegue validar mais aquela informação.

E outra coisa importante, se eu configurarei essas duas ROAs aqui, basicamente qualquer outra coisa que eu configure aqui não vai fazer diferença. Por quê? Porque uma vez que uma das ROAs valide qualquer anúncio, não dá para você invalidar mais. Então, se eu, por exemplo, quiser forçar aqui, esse /22 aqui, e eu não quero aquele /24. Aí eu vou falar assim: Não, eu vou adicionar uma ROA referente aqui a esse meu IPv4 /22, no máximo /22. Vamos fazer esse anúncio.

Aí ele fala aqui: Não dá para adicionar, porque ele já está sendo abrangido pela ROA anterior. Então o que acontece? Como aquela ROA, essa ROA aqui já engloba esse /22, ele não consegue... tudo que estiver aqui vai ser considerado válido. Não dá para você invalidar mais alguma coisa que já foi validado por uma ROA. Então, se eu quiser invalidar um anúncio, eu vou ter que retirar essa ROA aqui e inserir as ROAs específicas. Então, se eu inserir essa ROA mais abrangente, basicamente eu só vou ter essas duas ROAs mesmo, e não vai ter muito mais o que fazer. Por quê? Porque o /48 tende a ser o anúncio mais específico em IPv6, e o /24 é o anúncio mais específico que eu tenho em IPv4. Então, não é esperado na internet que venha anúncios /25, e nem coisas mais específicas que /48.

Então, basicamente, não tem muito mais o que fazer. Então essa configuração aqui, ela é a mais segura porque não tem como você errar. Então se você, de repente, tiver outros anúncios que você queira fazer no futuro, não vai precisar mexer aqui na ROA, só que você tem que lembrar que qualquer anúncio que esteja de acordo com essa condição aqui, vai ser validado pelo RPKI, tá? Então só a ROA válida consegue validar ou invalidar as rotas. Então isso é uma coisa importante. Se morreu o servidor aí, de repente, eu não percebi, e essas ROAs, elas expiraram, e aí, o que acontece com o meu provedor? Não vai acontecer nada. O que vai acontecer é que na hora que você for validar vai falar assim: "Tem alguma ROA falando alguma coisa sobre você?". Aí ele vai falar que não tem. Então seria como se não estivesse usando o RPKI.

Então, se suas ROAs expirarem, você não vai ter problema nenhum. É como se você tivesse saído do RPKI. Então se você sair do RPKI, é como você estivesse na internet normal. Então ninguém vai te filtrar porque você não tem o RPKI. Você só vai ser filtrado se você configurou uma ROA errada. E aí, então, você configurou, aqui, por exemplo, só o /22 e você tem o /24, esse /24, vai ser invalidado pelo RPKI e você vai ser filtrado. Então só dá para você ter algum problema aqui se você especificamente colocar aqui, especificamente configurar uma ROA errada.

Então se você não tem segurança do que você quer, o ideal seria o quê? Que as suas ROAs sejam iguais aos seus anúncios do BGP. Se você... Se o seu anúncio muda muito, ou você não tem segurança com relação ao que você está fazendo, você pode colocar a ROA aqui abrangendo todos os anúncios.

No caso foi esse exemplo que a gente deu aqui. Uma ROA vai do /40 até o /48, se fosse um 32, né? Seria o /32 até o /48. E em IPv4, uma que vai lá desde o seu prefixo maior até o mais específico. Então você faz isso lá para todos os seus anúncios e você não precisa mexer mais. Só precisa lembrar de deixar essa máquina ligada sempre para o registro continuar validando essas informações e renovando os certificados. Tudo bem?

Então, pessoal a parte de configuração do Krill basicamente é essa. Uma vez que você configurou as suas ROAs o seu RPKI está pronto. Isso aqui está fazendo apenas com que as ROAs façam parte lá da base do RPKI para as pessoas que forem validar isso no futuro, tá? Aqui a gente não está falando de validação. Aqui só está falando de publicação. Validação é um processo separado que usa outros softwares e outros equipamentos. Então, veja que para fazer a configuração do Krill, a gente não usa nenhum roteador. Então não precisa configurar roteador nenhum aqui, né? É puramente feito aqui pelo servidor e pela interface Web. Então aqui não envolve comunicação com roteador. A validação, aí sim, você precisa ter um validador, que é um servidor com algum programa validador instalado, e o roteador que vai fazer lá, vai receber essa base do RPKI e vai validar as rotas que ele conhece.

Aqui na parte da publicação não precisa disso. Então aqui a gente está divulgando para internet as ROAs que a gente conhece. Tudo bem?

Então, pessoal, essa era a experiência de hoje. Eu espero que vocês tenham conseguido também acompanhar, e quem quis fazer junto, né? É basicamente essa configuração. Não tem muito segredo, vocês viram que é bem simples, na verdade, de configurar aqui a o Krill, né? Acho que muita gente tem medo de mexer nessas configurações. Mas a parte de instalação e configuração do servidor, ela é bem simples. Mesmo a parte de autorizar, está lá com registro, né? Basicamente é um copia e cola de XML. A parte realmente importante, que tem que tomar cuidado, é aqui na parte das ROAs.

Então, o ideal é que você saiba o que você queira publicar no RPKI. Se você não souber, pode colocar aqui o seu bloco inteiro. Que aí, pelo menos, não importa o que você anuncia pela internet, ele sempre vai ser validado. Então é muito da escolha do provedor.

Você pode também começar com um anúncio desses, e, conforme você se sentir mais seguro, você mudar os anúncios aqui. Se você tiver problema... Assim, então alguém está sequestrando o seu bloco, e você quer fazer uma publicação aqui para invalidar aquele bloco, provavelmente vai demorar um pouco, né? Por quê? Porque tem essa questão do delay, né? Até o registro receber aquele certificado e tem... o validador também tem Um tempo que demora para ele atualizar essa base. Então não vai ser imediato. Vai ter pelo menos uma meia hora deve demorar até essa informação ser propagada totalmente.

Então também tem que ter isso em mente. Se você quer usar RPKI de forma ativa, assim, para proteger contra um ataque imediato, talvez tenha ferramentas melhores para isso. Mas funciona. Só vai levar um tempo até tudo isso ser propagado. Tudo bem?

Então, pessoal espero que tenham aproveitado aí. E agora a gente vai ter um tempinho para tirar dúvidas de vocês. E então fiquem à vontade para perguntar. A ideia aqui é para que vocês realmente possam aprender. E que isso fique claro, como é que eu posso mexer na configuração. O que isso faz do meu lado. Quais os problemas que eu posso ter.

Então, fiquem à vontade para perguntar aquilo que vocês não entenderam ou que a gente não falou, mas que você considere importante, pode falar também. Tá ok?

Então é isso, pessoal. Obrigadão aí. E agora a gente começa, então, a parte de perguntas.

**SR. EDUARDO BARASAL MORALES**: Bom, agora que o pessoal já viu como fazer a instalação do Krill, trabalhar com o Krill, a gente vai para parte de perguntas. Mas antes, eu queria dar alguns avisos. Se você quer o certificado da live, de que você participou, trabalhou junto com a gente, se inscreve no link que a gente vai colocar agora no chat. Então dá uma olhada lá e se inscreve, e aí você vai ganhar o certificado. Esse certificado vai ser da live e você pode se inscrever até às 14h. Depois disso, a gente vai fechar as inscrições e não vai dar para inscrever mais. Então fique atento, já começa ali a se inscrever para não perder essa chance de ganhar o certificado.

Além disso, agora a gente vai colocar também um formulário de avaliação. O que você achou dessa live por enquanto. Então eu gostaria de pedir para vocês preencherem esse formulário de avaliação. Esse daí é só para a gente saber o que a gente pode melhorar, se a gente deve continuar fazendo esses eventos.

Então, por favor, é muito importante que vocês escrevam para a gente o que a gente pode fazer. Então vamos estar colocando o formulário de avaliação com o QR Code, comecem a preencher.

E já vamos para parte de perguntas. Então já podem escrever no chat as suas dúvidas, que a gente vai ler e vai responder na medida do possível, tá?

Então só um minutinho para vocês verem o QR Code, vão preenchendo o formulário de avaliação. Duas perguntas, uma é a nota da live e a outra é o que pode melhorar. Então a gente tem aí a nossa semana de capacitação. A primeira vez que a gente está fazendo isso, um tutorial ao vivo. Uma semana inteira de tutoriais. E a gente quer saber se vocês estão gostando, e a gente pode fazer mais outras vezes. Então é importante para a gente saber o que vocês já acharam desse primeiro dia. Mas, também, lembra, tem terça, tem quarta, quinta, sexta todos tutoriais diferentes. Então, não deixem de assistir nos próximos dias.

Então vamos dar uma olhada nas perguntas, né? Aqui a gente já separou algumas delas. A gente viu que vocês estão interagindo bastante. A gente viu que o pessoal realmente está interessado no assunto. E é importante que a gente divulgue o RPKI, porque a gente precisa utilizar isso para a gente diminuir os ataques na internet. Principalmente uma parte dos ataques.

E essa primeira parte do tutorial a gente falou só da questão de publicação. Por quê? Porque a segunda parte é validação. A gente teria que ter mais ali umas três horas para falar sobre esse assunto.

Então só falando, não adianta a gente pensar em validar se não tiver nada publicado. Então, a primeira parte é importante todo mundo começar a publicar os ROAs para a gente ter algo para poder validar. E, aí, depois a gente vai ver o que está válido, o que está inválido, vai descartar e vai colocar os nossos filtros. Então, por isso que a gente decidiu focar nessa primeira parte de publicação.

Então, tem uma pergunta do Jadiel Mota: "Tem uma lista de provedores cadastrados habilitados a trabalhar com o RPKI Brasil?". Inclusive é legal de a gente mostrar também uns links também, além desse que você está pedindo, Jadiel, mas que do BGPmon, do Whois, do Looking Glass, que você pode verificar as rotas.

E aí eu vou chamar a Erina para falar sobre esse assunto. Erina, fique à vontade.

**SRA. ANDREA ERINA KOMO**: Bem, deixa eu ver se eu consigo compartilhar aqui a minha tela. Ah, acho que foi.

Bem então já respondendo à pergunta. Tem uma base aqui, essa pasta é acessível. Ela está disponível via aí FTP. Então vocês podem acessar esse link: ftp://ftp.bgp.net.br/rpki. Vocês vão chegar aqui nesse repositório, e aí tem uma lista aqui de vários arquivos diários. Eu abri aqui já o arquivo que foi gerado ontem. E tem uma listazinha de ROAs que já foram publicados aqui no RPKI do Brasil. Vocês podem ver a AS, qual prefixo que foi anunciado. Então, já respondendo à pergunta, tem isso daí disponível, você já pode ver em quem já está anunciando ROAs aqui no RPKI brasileiro.

E, como o Eduardo comentou, tem algumas outras ferramentas interessantes de a gente comentar, que o pessoal pode usar, para verificar esse quesito do RPKI. Eu vou abrir aqui meu terminal.

Como ele falou, tem como você consultar no Whois, no caso do BGPmon, eles disponibilizam isso, eu vou consultar o endereço do NIC. E aí ele mostra aqui, RPKI status ROA validation successful. Então, tem uma ROA validando aquele endereço. Aí ele fala do AS 22548, que é do NIC. E tem um outro comando aqui também disponível para você consultar a ROA em específico, daquele prefixo.

Então ele fala o período de validade daquela ROA, qual é o trust anchor aqui, a âncora que está validando isso, que no caso aqui é do registro. Ele fala que o prefixo vai do /32 a um /48. Então, acho que a gente vai colocar esses comandos também lá no site da semana de capacitação, para depois vocês poderem consultar.

Além daqui disso, tem alguns Looking Glass que também disponibilizam essas informações. Então no caso aqui abri o Looking Glass da G8, e fiz aqui a consulta também para aquele mesmo endereço, IPv6 do NIC, aqui no BGP V6. Tem as várias opções aqui do BGP, e eu coloquei para testar. Ele retorna aqui, o prefixo validado via RPKI, então está ok.

Além desse Looking Glass da G8 tem um outro aqui da Telia Company. Eles também disponibilizam, você seleciona aqui o BGP, coloca ali o prefixo. Eu coloquei no caso aqui o IPv4 do NIC.br também, e coloquei para rodar. Aí ele fala que tem uma ROA válida para esse prefixo. Tem validação RPKI com communities.

Então vocês podem usar também essas ferramentas para verificar tanto os anúncios de vocês quanto outros anúncios que vocês queiram consultar de outras entidades.

Um detalhe importante, que assim que vocês terminarem o passo a passo, que nem o Tiago mostrou ali, e fizerem o anúncio da ROA, essa informação não vai estar automática já disponível para você consultar aí. Tem um tempinho de propagação dessa informação na rede. Então você tem que esperar um pouquinho para conseguir ver as suas informações, tanto aqui nesses Looking Glass, quanto ali no Whois que eu mostrei, ou aqui nesse banco de dados que eu falei, que é gerado diariamente. Então você vai ter que esperar um pouquinho, mas depois você pode fazer essa consulta.

Então fica essa dica para vocês, como vocês podem verificar e validar. Vocês podem usar esses vários sistemas que estão disponíveis, para fazer esse tipo de validação.

Bem, devolvo a palavra para o Eduardo.

**SR. EDUARDO BARASAL MORALES**: Muito bom, Erina. Realmente esses links vão ajudar o pessoal. Inclusive, tem outros tutoriais que o pessoal está escrevendo, tem um do Rafael Galdino, que também vale bastante a pena dar uma olhada. Está bem detalhado.

E é importante a gente trabalhar para ter mais o RPKI implementado aqui no Brasil. A gente mostrou lá o graficozinho, o Brasil está com verdinho bem claro. Lembra lá que ainda falta muito para a gente trabalhar e publicar.

Bem, vamos lá para outra pergunta? Tem aí uma pergunta do Breno Bilhar relacionada a esse... "Existe somente o Krill para o RPKI, né?". Então eu vou chamar agora o Tiago para falar sobre esse assunto. Tiago, fica à vontade para falar.

**SR. TIAGO JUN NAKAMURA**: Alô? Então existe um outro software que a gente tem, que é o chamado toolkit do Dragon Labs. Lá no slide deve estar listado, que o Eduardo comentou. O que acontece? Hoje, basicamente a gente tem só os dois softwares para utilizar como servidor delegado do RPKI. O Krill, é o que a gente escolheu para utilizar no próprio Registro. Então tem uma estabilidade e uma confiabilidade boa o suficiente para a gente utilizar em termos de produção. Quando pessoal da Dragon Labs lançou o serviço lá do delegado deles, era mais como uma prova de conceito mesmo, para ver se eles conseguiam, se era possível fazer esse modo delegado.

Então, se alguém conhece algum software que o pessoal tem utilizado com sucesso pode colocar no chat também. Mas do nosso conhecimento, basicamente são esses dois softwares só que você consegue utilizar para subir no servidor Krill, o servidor RPKI, o Krill ou o toolkit do Dragon Labs.

**SR. EDUARDO BARASAL MORALES**: Muito bom, Tiago. Realmente é legal de a gente comentar de outras ferramentas. Legal também de falar do modo hospedado, modo delegado. Aqui no Brasil a gente só tem essa questão do modo delegado, que você tem que trabalhar com o Krill e conversar com o Registro. No modo hospedado, que tem no Lacnic, que tem em outras regiões, você pode entrar lá no sistema do Lacnic e trabalhar criando ali seus ROAs.

Mas aqui, por enquanto, a gente tem que trabalhar com o modo delegado. Então tem que instalar o Krill, mexe lá no Lagosta e faz publicações dos seus ROAs.

Bom, indo ali para outras perguntas tem do Basconan: "Entendo que em um service provider é superimportante implementar o RPKI. Mas e no cliente final que tem ASN, seria necessário implementação de RPKI? Não seria muito complexa a sua administração?". Então eu vou chamar agora a Erina para responder essa pergunta. Erina, fique à vontade.

**SRA. ANDREA ERINA KOMO**: Bem, então, como eu tinha comentado durante a apresentação dos slides, tem duas formas que pode ser feito o anúncio dos prefixos desses clientes no RPKI. Uma opção é você... Ah, você recebeu ali um certificado digital do NIC.br, e você vai gerar um certificado digital para o seu cliente criar mais um nível naquela cadeia de hierarquia de certificação. Aí, no caso, o cliente vai ter que fazer a geração das chaves dele, as ROAs dele. Que nem você fez para o seu AS, ele vai fazer lá para a situação dele. De fato, isso pode ser, talvez, um pouco mais complexo administrativamente para o cliente.

Então, uma oposição seria, ao invés de você gerar mais esse nível na cadeia de certificação, você mesmo fazer os anúncios das ROAs com as informações dos IPs que ele está usando. Se ele tiver um AS próprio, você pode gerar ali com o AS dele aquela ROA, e você vai assinar essa ROA, porque você também... O NIC.br falou que você tem o direito ali de usar aquele bloco de endereços.

Então você pode fazer dessas duas formas. Ou você mesmo cria a ROA para aquele seu cliente, ou você passa essa parte de administração para o seu cliente, e você pode conversar com ele e ver o que os dois

ficam mais confortáveis de fazer em relação a isso. Espero ter sido clara. Então devolvo a palavra para o Eduardo.

**SR. EDUARDO BARASAL MORALES**: Não, muito bom. Se pessoal não entender, escreve de novo a pergunta que a gente lê de novo, tenta explicar de uma maneira diferente.

Bom, eu tenho uma pergunta aqui do Renan Menezes: "Se um PTT tiver filtro com base no RPKI, tem como eu definir que apenas em peering, ou eu irei anunciar o /24?". Eu vou repassar agora essa pergunta para o Tiago responder. Tiago, manda bala.

**SR. TIAGO JUN NAKAMURA**: Então, a base do RPKI, ela não diferencia o que é peering, o que é trânsito, né? Uma base única. Então não dá para você colocar uma ROA e falar assim: Essa ROA só vale para PTT. Então isso não dá para fazer.

Então, o ideal é que, independente da situação, todos os seus anúncios que você divulga, tanto para PTT como para o seu trânsito, estejam englobados em alguma ROA. Mas você não consegue diferenciar via RPKI coisas que são peering e coisas que são trânsitos. Para o RPKI é uma coisa só.

**SR. EDUARDO BARASAL MORALES**: É isso mesmo. Então, pessoal, publica ROA para os anúncios que você está fazendo. Porque se não tiver uma ROA correspondente, ele vai ficar como aquela parte amarelinha do gráfico que a gente mostrou, é desconhecido. Então não vai ajudar ninguém. Por quê? Porque agora a gente está pensando o quê? Em descartar as inválidas. Só que o grande mundo já está o quê? Desconhecido. Então não está protegendo ninguém. Se todo mundo começar ali publicar os ROAs, a gente vai aumentar a parte dos válidos, se alguém cometer algum erro vai ser descartado a rota, porque ela vai estar na parte de inválido e o desconhecido, ele tende a diminuir, e, até, no futuro, quem sabe, a gente consiga ficar com quase tudo ali 100% dos válidos.

Então, indo para outra pergunta, tem agora do Leandro Silva. Ele manda lá: "Bom dia. Dúvida, quando somos trânsitos de outra AS que já esteja assinando, teremos mudanças apenas nos filtros ou teremos que ter alguma informação a ser inclusa para anúncios do cliente?".

Agora eu vou chamar a Erina para responder essa pergunta.

**SRA. ANDREA ERINA KOMO**: Bem, então, admito que essa pergunta me deixou um pouquinho confusa. Então eu vou começar falando duas coisas. Em relação ao anúncio. Como assim anúncio? Aí, no caso dessa história toda do RPKI são dois anúncios. Tem o anúncio do que você vai colocar ali nas ROAs, no RPKI, e tem o anúncio que você vai fazer dos prefixos no BGP. Essas coisas são à parte.

Se o seu cliente... Você é provedor de trânsito, aí tem o seu cliente, ele já tem AS dele. Em relação ao BGP não vai mudar nada, o seu anúncio vai continuar daquele jeito. Já no caso para o anúncio no RPKI das ROAs, é o seu cliente que vai fazer esse anúncio e assinar ali digitalmente aquele documento, aquela ROA, e isso vai ficar publicado no repositório que vai ser consultado.

Então essa diferença, entre o anúncio, não sei qual anúncio específico você estava querendo dizer, mas para o seu BGP, o anúncio no BGP não vai mudar, né? O cliente vai fazer o anúncio da ROA e o anúncio no BGP vai ser mantido daquele jeito. Você vai repassando a rota.

Aí, em relação a filtros, você pode aplicar os filtros em relação às informações que estão disponíveis ali no repositório do RPKI. Então você pode fazer aquela validação para que ninguém anuncie ali aquele prefixo no lugar do seu cliente. Aí tem essa opção. Não sei se era bem isso, mas espero ter sido clara.

Então devolvo a palavra.

**SR. EDUARDO BARASAL MORALES**: É, eu acho que às vezes pessoas estão confundido um pouquinho com o IRR, que tem lá o AS7. O RPKI, pessoal, aqui a gente está fazendo a validação da origem, não é do caminho todo do ASPF. Ou seja, todo o trânsito tem que ir lá marcar informação, e a gente válida o caminho inteiro. Não. A gente está em um primeiro passo. Primeiro passo é o quê? A validação da origem. Então, o restante do caminho não está validado. Então a gente está validando só origem. Até porque se validasse tudo na cadeia, seria uma coisa mais complicada. Ia dar muito mais trabalho. Mas validando a origem, a gente já evita muitos dos problemas.

Então, a questão de você ser o trânsito e a pessoa lá, o seu cliente, está trabalhando com AS dela, com o ROA dela, não vai impactar na sua parte. Por quê? Porque nessa parte ali de publicação do ROA não tem ali uma relação assim: "Eu sou trânsito tal, eu sou trânsito do outro". Isso aí é mais questão do IRR, tá? Questão lá de AS7, ou então ali você quer marcar essa informação no próprio site do Registro. Lá tem o Whois, você pode marcar lá um pouquinho as informações de roteamento, tem peering db. Mas aqui, com o RPKI, a gente está só mexendo na parte ali da origem, tá? Então é bom ficar claro isso daí.

Tem uma pergunta também do Ricardo: "O BGP Hijacking é autorizado para serviços anti Ddos, o cliente contratou de mim o serviço, e preciso sequestrar o bloco. Mesmo com RPKI vão ser possíveis tais técnicas?". Então vou mandar para o Tiago responder essa pergunta.

**SR. TIAGO JUN NAKAMURA**: É, BGP Hijacking autorizado é um nome meio ruim. Mas eu entendi. A ideia é que você precise anunciar os blocos da pessoa, mesmo você não sendo o AS da pessoa. E isso dá para fazer sim. O RPKI, lembra? O que está bloqueado via RPKI é o anúncio daquele AS, tá? O número de AS, a pessoa consegue setar ali na configuração de RPKI dela. O que você não consegue é você fazer essa configuração para ela. O cliente vai ter que fazer essa configuração lá no sistema dela, no Krill dela, né? Ela vai precisar setar que você, como AS, é um AS válido para anunciar aquele prefixo dele, tá?

Então se você precisa, ter alguma situação em que você precisa anunciar o prefixo daquele cliente, dá para fazer, só precisa lembrar que a pessoa vai ter que fazer essa configuração no Krill dela, e ela vai ter que setar ali o seu AS para o bloco que você quer anunciar.

**SR. EDUARDO BARASAL MORALES**: É isso mesmo, Tiago. Então, pessoal, lembra, se você quer fazer esse roubo de prefixo autorizado que o pessoal está comentando, na verdade, é você dar a permissão para o outro anunciar o seu bloco. Não é um roubo, né? Fica uma coisa bem estranha.

Vamos para outra pergunta? Ricardo Holanda: "É obrigatório todas as empresas terem implementado o RPKI?". Aí eu passo para a Erina responder.

**SRA. ANDREA ERINA KOMO**: É então, né? Obrigatório pode ser uma palavra um pouco forte. Mas quando a gente mostrou aqui, nesse tutorial a gente está tentando falar isso, o RPKI, assim como o BGP, tudo, só funciona com a cooperação de todo mundo. Então todo mundo tem que participar, ajudar e colocar para funcionar de verdade.

Então não. Ainda não é obrigatório. A gente não manda você colocar o RPKI. Mas a ideia é que todo mundo comece a colocar os anúncios no RPKI e fazer as validações para melhorar toda segurança da comunicação na rede. Então é importante essa união de todo mundo. Então todo mundo ajudando para melhorar a internet.

**SR. EDUARDO BARASAL MORALES**: É legal também de comentar do MANRS, que a gente falou durante as apresentações. Não é uma obrigação, mas é legal que é quase um selinho de que você faz as coisas corretas. Então, se você está trabalhando com RPKI, está trabalhando com as outras informações de segurança no roteamento, assina o MANRS, tá? E aí mostra para o mundo que você aplica as boas práticas. Mas não pode ser só assinar uma vez, arruma tudo a casa, fica tudo certinho, e depois para frente esquece o RPKI esquece tudo, como se tudo estivesse rodando tranquilamente.

O RPKI é uma coisa que tem que ser mantida. Ela tem que ficar sempre sendo olhada. Se você muda os anúncios, tem que ficar ali mudando os ROAs. Não pode ficar ali, configurar e largar. Porque a gente vê muito provedor também fazendo isso, configura e larga. Acha que vai funcionar aquilo para sempre, uma vez feito, não precisa mexer mais. Não é assim. Então tem que sempre cuidar e manter.

Então a gente fala do MANRS, fala que é uma iniciativa muito boa. A gente comenta que os provedores devem assinar. Inclusive aqueles que contratam provedores devem começar a exigir que o provedor assine o MANRS. Então a gente fala até de governo, falando ali de licitação, lembrando: "Oh, quero contratar um provedor para me prestar serviço". Esse provedor tem que estar com as seguranças corretas, as normas de segurança feitas. Então eu quero que ele assine o MANRS. Então, a gente quer o quê? Ver mais brasileiros, mais provedores trabalhando com o MANRS.

Como a Erina mesmo comentou, é uma questão de cooperação, todo mundo tem que trabalhar em conjunto. Adianta você validar sozinho, sendo que ninguém publicou? Não adianta. Não tem informação. Vai ficar tudo como desconhecido.

Adianta ali você publicar e ninguém validar? Também não adianta. Por quê? Porque vai todo mundo aceitar as rotas independente de ter ali um ROA ou não.

Então, a gente precisa trabalhar duas partes em conjunto e todo mundo tem que fazer. Não é obrigatório. Mas pensa que isso vai evitar problemas para você e vai evitar problemas para os outros. Se você publica o seu ROA colocando ali do seu prefixo, que você está utilizando, e o pessoal já valida, aquilo vai evitar que roubem o seu prefixo. Entoa essa primeira parte já via te ajudar nesse quesito, se alguém digitar alguma coisa errada, tentando roubar o seu prefixo, você já vai estar uma parte protegido.

Depois disso, você vai trabalhar com a parte ali de validação, que você vai receber as informações dos outros e vai dizer se estão corretas ou não estão corretas, se você aceita ou não aceita essas informações. Isso aí vai te ajudar na questão de alguém que roubou algum prefixo, mande aquela informação para você, e você não mande tráfego para aquele prefixo roubado. Porque aí os seus clientes também estão sendo afetados, eles queriam acessar determinado site e não estão acessando. Por quê? Porque está indo no caminho errado, porque alguém roubou o prefixo, alguém vazou uma rota. Então, você está sendo penalizado da mesma forma.

Uma coisa que eu gosto de ressaltar, porque surgiu em conversa de provedores, não façam a lei antiga do olho por olho, dente por dente. Alguém roubou o meu prefixo, eu vou lá e roubo o dele. Isso daí é uma coisa, assim, absurda. Não é porque alguém fez algo errado, você deve fazer algo errado também. Então às vezes a pessoal nem pensa no RPKI, que pode ajudar ele, já pensa assim: "Ah, roubou o meu, eu vou roubar o dele. Vou atacar ele para ele ver que ele está fazendo coisas errada".

Então, não pensem isso, é errado, prejudica para internet como um todo. Você, roubando um prefixo, está sendo prejudicado, porque vai vir tráfego para você, ou seja, vai usar o seu trânsito e pode ser que você

não aguente, vire ali um ataque de autonegação de serviço. E aí você fica fora e todos seus clientes ficam fora.

Então, nem pense nisso. A gente vê em grupo de provedor o pessoal comentando. É um absurdo. Então vamos trabalhar com normas de segurança corretas. Então, apliquem o MANRS, apliquem o RPKI, que é uma parte do MANRS, e vai ajudar bastante vocês.

Então vamos lá para outra pergunta, né? Tem do Amir Alves de Paiva: "Como ficaria a questão dos provedores que não são trânsito? O meu provedor de trânsito, ele poderia repassar para mim apenas os prefixos validados?". E aí eu vou chamar o Tiago para responder essa pergunta.

**SR. TIAGO JUN NAKAMURA**: Acho que uma coisa importante de lembrar é que a publicação que a gente está fazendo via Krill não tem nada a ver com a validação. São processos independentes, tá? Então o que eu estou publicando ali, não vai ser magicamente filtrado, na internet. Isso é filtrado, porque do outro lado, os provedores precisam validar essa informação usando algum software validador, tá?

Então é o que Eduardo comentou: lá você pode usar Routinator, OctoRPKI, o Fort. Tem vários programas que fazem essa validação. Mas ela tem que ser feita. Então não é automático. Eu publiquei a ROA, não é magicamente as coisas são filtradas, tem o lado da validação que também precisa ser feita para que o RPKI funcione.

Para essa validação funcionar, a gente precisa ter tanto o validador como a conversa desse validador com o roteador. Que tem que conversar via protocolo RTR.

Lembra que a gente falou que o Mikrotik não suporta o RTR, né? E o pessoal pergunta: "Como é que eu posso filtrar a minha rota do RPKI, se eu não consigo comunicar via RTR?". Uma solução é, de fato, você pedir para o seu upstream, para o seu provedor fazer esse filtro para você. Então ,se ele já entregar a tabela BGP filtrada, você não precisa se preocupar em revalidar aquilo via RPKI.

Outra opção, se você não quiser receber tudo filtrado, porque às vezes o cara filtra coisa a mais, você pode pedir para ele setar uma community para você de RPKI válido, inválido ou desconhecido. Daí ele: "Seta três communities para mim, um para cada tipo de validação de RPKI". E aí, dentro do seu provedor, você faz o filtro, não via RPKI, mas via Community. Então também dá para fazer isso.

Então tem várias formas de você conseguir filtrar o RPKI da tabela BGP. A mais ideal seria ter um validador próprio. Mas, se não der para ter um validador próprio, é uma possibilidade você pedir para o seu trânsito fazer esse filtro para você.

**SR. EDUARDO BARASAL MORALES**: É, bem lembrado que tem roteadores que têm essa dificuldade de falar com o validador. Então você fala com o seu upstream, e pede para ele mandar para você, por exemplo, com communities ou fazer o filtro para você. Com community, o pessoal fala para marcar, porque aí, pelo menos, você toma a decisão em cima do tráfego que você está recebendo. Pode ser que no momento você não queira filtrar, você queira só diminuir o local preference. Então é possível.

Então, eu quero ver o quanto que o RPKI vai me afetar em uma validação. Pode ser também uma ideia. Que a gente fala assim, com communities você pode ver quantas rotas ali você invalidaria se você colocasse ali um filtro... Quer dizer, quantas rotas você descartaria por estarem marcadas inválidas. E aí você pode ver o impacto que poderia te causar talvez alguém cometendo algum erro.

O que a gente vê é que realmente as inválidas, elas prejudicam, porque estão recebendo muitas rotas que não deveriam ter sido enviadas, e o melhor seria descartar. Mas, está com medo? Atua com uma medida um pouquinho mais tranquila.

Bom, tem uma outra pergunta do Ronilson José: "Qual o recurso que a máquina poderia ter para levantar o Krill?". Então eu vou passar para Erina responder essa pergunta.

**SRA. ANDREA ERINA KOMO**: Bem, então acredito que não precisa ser uma máquina, assim, tão potente, né? O Tiago mesmo, quando ele montou ali o tutorial, ele falou, colocou no Linux, uma máquina virtual no computador dele.

Então não deve precisar demandar muito processamento e nem memória. O pessoal da equipe que criou ali o Krill, o pessoal da NLnet Labs, eles fizeram testes, eles falaram que dava para subir o servidor Krill em um Raspberry Pi, por exemplo. O importante é, você precisa manter essa máquina sempre ligada, sempre de pé. Como a gente falou, ela vai ficar trocando ali comunicação, atualizações automáticas com o servidor Krill do NIC, do Registro.Br.

Então, é importante, mesmo que você suba aí: Ah, vou colocar em uma máquina virtual e um servidor aqui, vou subir o servidor Krill. É importante que fique sempre ali acessível, não precisa gastar tanto processamento e nem memória. Mas ele tem que ficar sempre ligado. Então, não sei especificamente certinha. Eu sei que não precisa de muito recurso.

**SR. EDUARDO BARASAL MORALES**: Tem uma outra pergunta aqui que pode ajudar a responder essa daí. Porque ela também fala do servidor Krill, e aí eu passo para o Tiago.

Então, o Milton Oliveira Vieira: "O servidor Krill deve estar conectado diretamente à internet, sem uso de NAT? Ou é possível usar atrás de NAT]? Senão ele vai ficar pegando com IP privado ao invés de IP público". Então, acho que seria legal, Tiago, você complementar com a resposta da Erina sobre o servidor.

**SR. TIAGO JUN NAKAMURA**: É, no site lá do Read The Docs, do Krill, que eu usei no tutorial, ele tem toda a especificação das configurações mínimas e dos sistemas operacionais que eles testaram. Não quer dizer que não funcione em outras configurações. Até porque o código, ele é open source, né? Então dá para você tentar instalar ele em outras circunstâncias que não foi testado ali para eles. No caso do NAT, dá sim, para configurar o Krill atrás de NAT.

Inclusive, nesse tutorial, eu estava... aqui, na minha máquina, eu fiz atrás de NAT. Aliás, eu fiz atrás de dois NATs, porque eu estava com o NAT da máquina virtual e o NAT do roteador de casa. Então funciona. Porque o UpDown, ele sai do nosso cliente Krill para o servidor Krill lá do Registro. Então não tem problema. Mesmo que o seu servidor esteja atrás de NAT, ele consegue se comunicar lá com o Registro.Br. Então não tem problema, por exemplo, fazer numa rede 'nateada'.

**SR. EDUARDO BARASAL MORALES**: Bom, só para comentar uma discussão que teve calorosa no chat, que foi a questão do black hole, de como que poderia se tratar essa situação. Ainda assim, não tem uma regra muito bem específica ou bem divulgada com a questão do communities do black hole, que o pessoal anuncia /32, afinal, quer anunciar uma parte que está sendo atacada para ser descartada. E, no caso ali, você deveria fazer o ROA do seu prefixo até o prefixo máximo do 32, do 22 ao 32? Não, não deve fazer isso. O que a gente geralmente fala é que você deve trabalhar com os ROAs em cima dos prefixos que você atua para fazer ali roteamento naquele momento. Então você vai trabalhar com os 22, os 24, não ali até o /32, dando todo range. Por quê? Porque nesse caso você está permitindo o próprio erro do seu

administrador de rede. Por quê? Porque se ele digitar alguma coisa errada, /26, o ROA vai dizer assim: "Ah, está válido". Então o outro upstream vai aceitar e assim por diante, assim por diante. Se ninguém botar filtro do /25, você está propagando rota que também não deveria existir na internet, rota lixo. Então tem que tomar cuidado, tá?

Então não... colocar um range muito grande. O que a gente tem visto mundo afora é que o pessoal não recomenda fazer isso. Mas aí, como fica o /32? Afinal, ele vai marcar como inválido se você coloca entre 22 e 24. Então, o 32 ele realmente ali é um problema nessa questão do black hole, você marca a community lá, e aí ele mostra inválido, e você toma a decisão de descartar aquela rota. Só que, na verdade, você está mandando aquela rota para que ele descarte o tráfego, não descarte a rota em si.

O que a gente vê de solução, né? O que podemos ali recomendar? Que você trabalhe esse filtro da community antes de trabalhar o filtro do RPKI. Então você pega ali o /32, e coloca ali, ou seja, aponta o next hope para o lixo, aceita ela, e aí você começa a descartar o tráfego. E depois você pega ali as outras rotas enviadas e você faz ali a validação do RPKI e acaba descartando as rotas que você não quer, as inválidas.

Então você toma atitude prévia. Você pega ali as rotas, coloca ali com uns mats(F) para ver essa questão da community do /32.

Então, ainda não tem uma grande recomendação sobre isso. Tá? Mas pessoal lá do IETF está trabalhando, outros operadores de rede estão comentando, e aí, em breve, quando surgir alguma coisa, a gente vai publicar para vocês e divulgar amplamente, para vocês trabalharem da melhor forma. Tá? Por enquanto é isso que a gente tem para falar.

Bom, vou passar agora para o Moreiras, dar uma conclusão final para nosso evento de hoje, e já chamando também para o evento de amanhã. Então, Moreiras, fique à vontade.

**SR. ANTÔNIO MARCOS MOREIRAS**: Bom, gente eu tenho alguns recadinhos finais para passar para vocês. E alguns comentários, até de alguns pontos que fui anotando aqui durante a live.

Primeiro ponto. Não sei se vocês repararam como a capacidade que o Tiago, o Eduardo e a Erina tinham, enquanto estavam dando as explicações, ainda assim, eles iam tirando dúvidas de vocês no chat. Impressionante essa capacidade, né, gente?

Na verdade, é que parte das explicações, parte da live nós gravamos previamente em vídeo. Por quê? Porque muitos de nós estamos fazendo home office, e corria o risco de a internet cair, de ter algum problema. Então, estava todo mundo aqui ao vivo, todo mundo aqui prestando atenção, essa parte final todos entraram ao vivo para falar com vocês. Mas alguma parte das explicações a gente tinha pré-gravada. Porque se tivesse algum problema sério com internet, a gente não ia deixar de ter a live por conta disso.

Eu achei que foi muito legal. Que o resultado foi legal. Se vocês acharam alguma coisa diferente depois vocês comentam com a gente. Por falar de comentar, o Eduardo já falou da avaliação, da importância da avaliação para a gente. Eu pedi like várias vezes aí. Tem mais de 500 likes o vídeo, apesar de ter 700 pessoas assistindo, podia ter um pouquinho mais de likes. Mais os likes são sinais que gostaram da live, gostaram do assunto técnico. Mas é importante para a gente que vocês respondam a avaliação. Uma avaliação curtinha, são só duas questões, para vocês darem uma nota lá de um a dez, e fazerem o comentário do que seria importante melhorar para as próximas lives.

Então é muito legal que vocês respondam. Porque dá a chance de a gente melhorar e entregar um conteúdo vocês no futuro.

Alguns comentários técnicos, eu peço para o pessoal do NIC.br colocar o link de novo da avaliação no chat para o pessoal. E colocar o link também da inscrição, quem precisar do certificado, quem quiser o certificado. Lembrando que tem até hoje, às 14h, para fazer a inscrição para receber o certificado. Porque ó certificado é para quem basicamente está acompanhando aqui online com a gente Depois o vídeo vai ficar disponível, tudo mais, para quem quiser assistir, quando quiser assistir, ótimo. Mas o certificado é para quem está acompanhando aqui online, ao vivo, com a gente.

Alguns comentários técnicos, né? Então é superimportante vocês lembrarem o que já foi repetido várias vezes, que o RPKI tem duas partes: Tem a parte que você criar seus ROAs, de você assinar seus prefixos ali com RPKI, e tem a parte de você fazer os filtros. São duas coisas independentes, mas as duas são extremamente importantes. Você tem que fazer as duas. Para o RPKI funcionar na internet como um todo é importante que as duas coisas estejam feitas. Aí o Tiago deu boas dicas de como fazer isso, até mesmo quando você tem roteadores que não suportam a parte de filtro ainda, né?

Um outro comentário que eu gostaria de reforçar é a questão do delegado versus hospedado. Até por algumas perguntas e comentários que observei no chat. O Lacnic começou o RPKI aqui na América Latina usando o modo hospedado. Muitos outros RIRs também começaram com o modo hospedado. Agora, o NIC.br começou, recentemente, no final do ano passado, e começou com modo delegado.

Por quê? Porque até pouco tempo a gente não considerava o RPKI uma tecnologia madura, ainda. Vocês veem que implantação do RPKI em toda a internet, ela está basicamente no início. O Lacnic foi pioneiro. Quando o Lacnic começou a oferecer RPKI, mal existiam softwares para você conseguir fazer o suporte RPKI. Não existia um software como o Krill, com essa interface bonitinha, que é o Lagosta, essa interface Web, que é superficial de instalar. O Tiago explicou muito bem. Superfácil de operar. Vocês veem que RPKI em si parece bastante complicado, cheio de detalhe, certificado, trust anchor, pipe, e o Krill vem e simplifica isso tudo. É muito fácil de você operar, é muito fácil de você instalar, muito fácil de você fazer funcionar.

Então a gente fica sabendo da teoria ali, por trás, para ter ideia de como aquilo funciona. Mas muito da complexidade disso é escondido pelo Krill. E o Krill não estava disponível até antes do final do ano passado. O Krill ficou disponível agora. E por isso que agora o Registro.Br começou a operar.

E o modo delegado, ele te dá mais controle. O certificado fica com você, o seu certificado. Isso de um ponto de vista de segurança, do ponto de vista de como o protocolo foi pensado, isso faz mais sentido do que o modo hospedado.

Então, não vejam isso como uma coisa ruim. Vejam isso como algo bom. O Registro.Br esperou o RPKI estar mais maduro, esperou ter softwares fáceis de usar, softwares maduros o suficiente para você poder instalar no seu provedor de uma forma fácil, seu consultor poder instalar e operar de uma forma fácil, para poder disponibilizar isso para você. E, agora é só implantar, né? Agora a coisa não é difícil. Tem esse tutorial, tem tutorial que o pessoal fez no final do ano tem... Como pessoal comentou aí, tem um tutorial lá no blog do Rafael Galdino, que também está bem legal.

Então tem muito aí. Com certeza vai surgir mais material por aí e vocês não vão ter dificuldade de fazer isso daí.

Um outro comentário é o seguinte, sobre IP e AS. Você... o teu provedor é uma organização e você recebe dois conjuntos de recursos de numeração lá do Registro.Br. Um, são os blocos de IP, outro é o número, o ASN, que você usa no BGP. São dois recursos de numeração diferentes que estão alocados para mesma instituição, para a mesma entidade que quer você provedor. São duas coisas independentes que normalmente andam juntas. E faz todo sentido de que andem juntas. Geralmente o IP e o ASN são alocados em conjunto, até em uma mesma solicitação. Porque você precisa do ASN para anunciar os IPs no BGP.

Agora, eles são coisas separadas. São coisas separadas. Você pode usar os seus IPs com ASN de terceiro. Foi uma das dúvidas que se apresentaram aí, o Eduardo já respondeu. Ou foi o Tiago que respondeu.

Mas é normal. Isso não é algo ilegal, você só precisa de um jeito de documentar isso para que os filtros funcionem direitinho. E o RPKI é uma dessas formas. O RPKI, geralmente ele dá ao detentor dos IPs uma forma de dizer qual ASN está anunciando aqueles IPs na tabela BGP. Normalmente é o próprio ASN do próprio detentor dos IPs, do mesmo provedor, da mesma entidade, entendeu? Mas pode ser um ASN, por exemplo, do seu stream provider, do teu provedor de trânsito, ou outro que pediu diretamente para anunciar parte dos teus blocos IP.

E um último comentário sobre a obrigatoriedade. A Erina respondeu bastante bem, mas eu gostaria de fazer um comentário extra. Nada na internet é obrigatório, né? Não tem uma entidade, internet não é um negócio regulado igual telecomunicações, não tem nenhuma entidade que te diz: "Olha, você é obrigado a usar IP. Você é obrigado a usar BGP". Tem? Não tem. Se você não quiser usar IP, você não precisa. Se você não quiser usar BGP, você não precisa. Só não vai funcionar, certo? Você só não vai conseguir se conectar com o resto da internet. Só tem esse detalhe, são coisas acordadas.

Mas daí você me fala: "Moreiras, mas se eu não usar o RPKI vai deixar de funcionar alguma coisa?". Hoje não. Porque está em implantação. Mas a gente já viu diversas redes importantes, CDNs, inclusive, falarem por aí em eventos, que em breve vão começar a filtrar todo mundo que não tiver RPKI válido.

Ah, vão fazer isso no curto prazo? Não, porque enquanto a maioria não estiver anunciando no RPKI, se alguma rede resolver filtrar o que for desconhecido, não vai funcionar. Vai ter muito problema. Então, provavelmente, não vão fazer isso tão rápido assim.

Mas já teve gente importante, redes importantes que prometeram fazer isso em breve, né? Então é interessante que todo mundo esteja com seus prefixos lá, com os ROAs válidos e tudo mais. Bom, era isso que eu queria comentar.

Eu quero agradecer a presença de todos. Quero agradecer muito o Eduardo, o Tiago, a Erina por terem feito tutorial, por terem... Também Eduardo e toda equipe, organizado essa semana de capacitação. Quero convidar todo mundo a estar presente aqui durante a semana inteira. Os tutoriais do resto da semana vão ser excelentes.

Temos tutoriais com a Juniper, Wztech, com a Icann, com a VLSM, com a Cisco nos próximos dias. Os tutoriais de quarta e quinta-feira, especificamente, tem uma parte prática. Vocês podem baixar com antecedência, máquina virtual, vocês vão poder acompanhar no trabalho de vocês, na casa de vocês, a parte prática do tutorial, quem quiser. Quem não quiser pode só acompanhar assistindo também. Fiquem à vontade.

E é isso, gente. Vamos encerrar a live aqui por hoje. Agradeço a todos. E a gente conta com vocês no resto da semana. Divulguem para os seus amigos, para os seus conhecidos, para os seus colegas de trabalho, para que eles também estejam aqui no restante da semana, caso tenham perdido o tutorial de hoje. Vocês foram sensacionais. Teve muita participação no chat, muitas perguntas inteligentes, interessantes, mostrou interesse muito legal. Foi muito legal participar dessa live e ver a participação de todos vocês aqui que nos acompanharam, tá? Muito obrigado. E até amanhã.