Guia de implantação de IPv6 para empresas

Edwin Cordeiro – NIC.br
ecordeiro@nic.br

O grupo v6ops do IETF

- O IETF é o local onde os protocolos e recomendações para a Internet são desenvolvidos
- O grupo v6ops tem como objetivo acompanhar a implantação do IPv6, gerar recomendações para uma transição bem sucedida, evitar que esta implantação gere redes segregadas e documentar problemas em protocolos ao adotar o IPv6

Enterprise IPv6 Deployment Guidelines

- Documento desenvolvido pelo v6ops, no momento seguindo o processo para ser publicado como uma RFC informacional
- Disponível integralmente e gratuitamente em: http://datatracker.ietf.org/doc/draft-ietf-v6ops-enterprise-incremental-ipv6/

Proposta

- 3 fases:
  - Análise, documentação e preparação;
  - IPv6 na interface com a Internet;
  - IPv6 na rede interna;
- Considerações adicionais:
  - IPv6-only
  - IPv4-only
  - Outros

Análise, documentação e preparação

- Como implantar IPv6 afeta várias áreas é importante ter o apoio executivo, não basta só a equipe de redes / sistema decidir fazer
- A preparação é importante para definir cronogramas, prioridades, troca de equipamentos, vulnerabilidades, fornecedores não compatíveis

Análise, documentação e preparação

- Fazer inventário de quais equipamentos possuem suporte IPv6 e se este suporte IPv6 possui equivalência de todas as funções usadas em IPv4
- Verificar se aplicações internas ou contratadas de terceiros possuem suporte IPv6
- Não basta ler no manual que tem suporte, é necessário testar e documentar os testes

- Em muitos casos, mesmo as equipes de redes e sistemas, não possuem conhecimento suficiente de IPv6, já que este muitas vezes não é incluído no escopo de universidades e cursos
- Projeto IPv6.br oferece treinamentos gratuitos, já foram realizados cursos dedicados para a FEBRABAN. Outros funcionários de bancos podem se inscrever nos cursos. Agenda disponível em: http://ipv6.br/calendario/

- "Se o IPv6 não estiver implementado na minha rede, posso ignorá-lo"
  - Adotar esta postura pode gerar sérios problemas para a sua rede
  - É necessário se preocupar com segurança IPv6 mesmo sem ainda ter IPv6 nativo em sua rede
  - Os sistemas operacionais atuais possuem suporte nativo a IPv6 e o IPv6 tem preferência de uso sobre o IPv4, muitas vezes criando túneis automáticos para isso

- A ausência de NAT em IPv6 é usada para dizer que o IPv4 é mais seguro, mas uma política de segurança em IPv6 com o mesmo nível de exigência que a do IPv4 iguala a segurança entre IPv4 e IPv6
- IPSec foi desenvolvido para o IPv6, mas o uso não é obrigatório, assim como não é em IPv4. Logo não é possível dizer que IPv6 é mais seguro por usar IPSec
- Existem diferenças entre os protocolos, verifique como elas impactam sua rede

Plano de Endereçamento IPv6

- Muda bastante com relação ao IPv4, onde a regra era a máxima economia
- Em IPv6 a regra passa a ser organização e agregação de rotas
- A alocação mínima recomendada para uma empresa é um /48, permitindo 65636 redes. Se seu provedor estiver oferecendo um prefixo menor questione. Se você for um Sistema Autônomo (AS) justifique a necessidade ao fazer sua solicitação de IPv6 ao Registro.br, de um bloco maior

IPv6 na interface com a Internet

- Conectividade: solicitar ao seus provedores de trânsito e configurar em suas seções de peering
- Segurança: firewall IPv6 deve ser equivalente ao IPv4. Note que ICMPv6 agrega novas funções com relação ao ICMPv4 e não pode ser totalmente descartado
- Configuração de servidores e aplicações: não basta só ativar IPv6 nas interfaces, muitas aplicações necessitam configurações adicionais, mudanças de logs e BDs, etc

IPv6 na rede interna

- Segurança: além de garantir equivalência a do IPv4 é preciso atenção ao mecanismo de Descoberta de Vizinhança (NDP), antes feito pelo ARP, agora faz parte do ICMPv6 e possui novas funções que podem gerar vulnerabilidades
- Infraestrutura: garantir que os equipamentos podem fazer em IPv6 tudo o que sua rede faz em IPv4. A distribuição de endereços pode ser feita via DHCPv6 ou NDP, com maneiras distintas de controle de acesso e alocação de endereços em cada protocolo

IPv6 na rede interna

- Dispositivos usuários: a maior parte dos sistemas operacionais suporta IPv6 e este suporte é habilitado por padrão, mas existem nuances entre os SOs que devem ser testadas na fase de análise
- Sistemas corporativos: todos os sistemas devem suportar IPv6, entre eles, email, video conferência, telefonia VOIP, DNS, sistemas de monitoramento etc

IPv6-only

- Hoje o mais comum é a utilização de pilha dupla nas redes, permitindo o crescimento gradual do IPv6 até ser factível desligar o IPv4
- Organizações muito grande podem não ter endereços IPv4 privados suficientes (RFC 1918) ou querer, em uma expansão, simplificar a rede com só um protocolo
- IPv6-only na rede interna é possível, mas mecanismos para se comunicar com redes sem IPv6 podem ser necessários, por exemplo, NAT64/DNS64

IPv4-only

- Mesmo optando por não colocar IPv6 em alguma parte da rede ele não pode ser ignorado, pois isto pode ser fonte de vulnerabilidades
- Se o IPv4-only for em servidores conectados na Internet é necessário garantir que os logs incluam IP e **porta** de origem, data e hora, pois o outro lado pode estar usando um IPv4 compartilhado via CGNAT

Outros

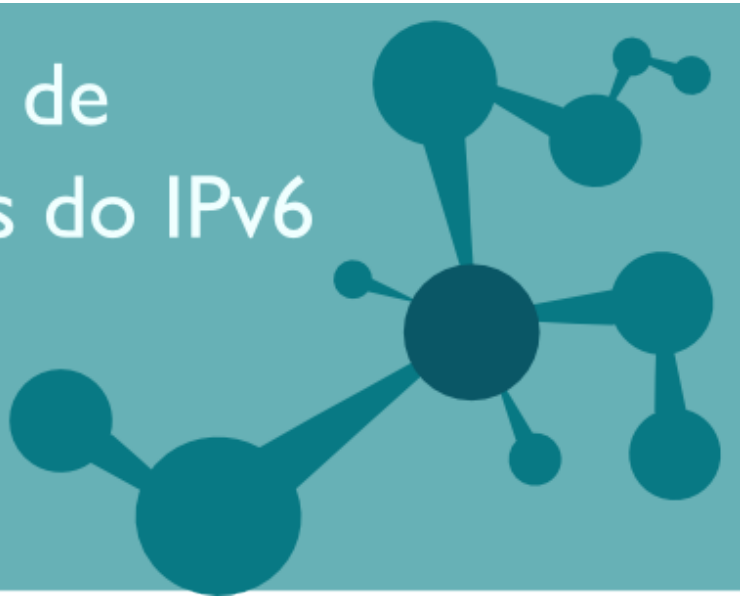
- O documento ainda aborda aspectos de Content Delivery Networks (CDN), Virtualização de Data Centers e Redes Universitárias
- Caso haja interesse nestes casos o documento pode ser consultado diretamente

Participe

IV Semana da Infraestrutura da Internet no Brasil

24 a 28 de novembro

Forum Brasileiro de Implementadores do IPv6



Quarta-feira
26 de novembro

- Perguntas?

- Edwin Cordeiro
  - ecordeiro@nic.br
  - ipv6@nic.br