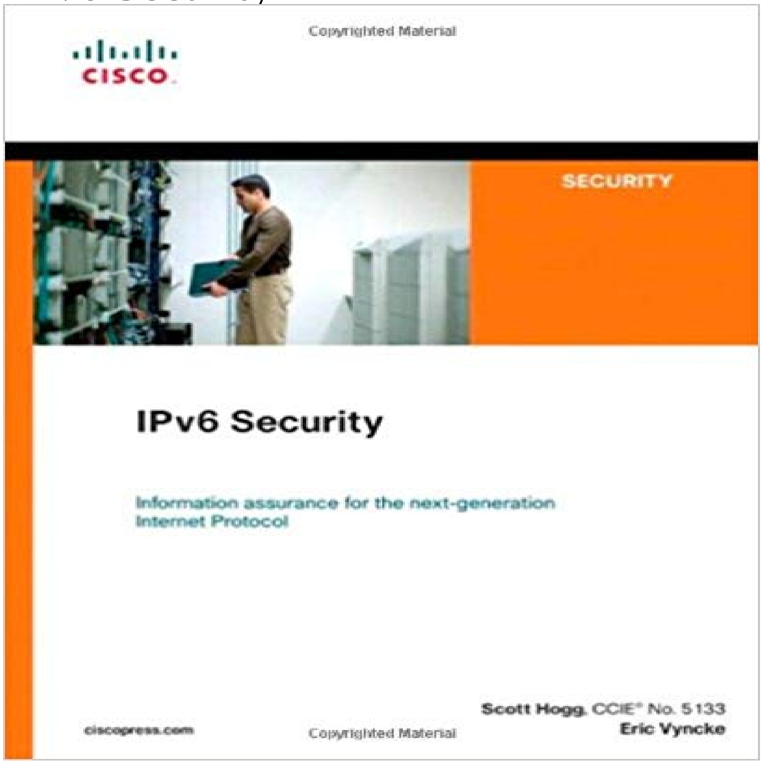
IPv6 Security



IPv6 Security Protection measures for the next Internet Protocol As the worlds networks migrate to the IPv6 protocol, networking professionals need a clearer understanding of the security risks, threats, and challenges this transition presents. In IPv6 Security, two of the worlds leading Internet security practitioners review each potential security issue introduced by IPv6 networking and present todays best solutions. IPv6 Security offers guidance for avoiding security problems prior to widespread IPv6 deployment. The book covers every component of todays networks, identifying specific security deficiencies that occur within IPv6 environments and demonstrating how to combat them. The authors describe best practices for identifying and resolving weaknesses as you maintain a dual stack network. Then they describe the security mechanisms you need to implement as you migrate to an IPv6-only network. The authors survey the techniques hackers might use to try to breach your network, such as IPv6 network reconnaissance, address spoofing, traffic interception, denial of service, and tunnel injection.

The authors also turn to Cisco products and protection mechanisms. You learn how to use Cisco IOS and ASA firewalls and ACLs to selectively filter IPv6 traffic. You also learn about securing hosts with Cisco Security Agent 6.0 and about securing a network with IOS routers and switches. Multiple examples are explained for Windows, Linux, FreeBSD, and Solaris hosts. The authors offer detailed examples that are consistent with todays best practices and easy to adapt to virtually any IPv6 environment. Scott Hogg, CCIE No. 5133, is Director of Advanced Technology Services at Global Technology Resources, Inc. (GTRI). He is responsible for setting the companys technical direction and helping it create service offerings for emerging technologies such as IPv6. He is the Chair of the Rocky Mountain IPv6 Task Force. Eric Vyncke, Cisco Distinguished System Engineer, consults on security issues throughout Europe. He has 20 years experience in security and teaches security seminars as a guest professor at universities throughout Belgium. He also participates in the Internet Engineering Task Force (IETF) and has helped several organizations deploy IPv6 securely. Understand why IPv6 is already a latent threat in your IPv4-only network Plan ahead to avoid IPv6 security problems before widespread deployment Identify known areas of weakness in IPv6 security and the current state of attack tools and hacker skills Understand each high-level approach to securing IPv6 and learn when to use each Protect service provider networks, perimeters, LANs, and host/server connections Harden IPv6 network devices against attack Utilize IPsec in IPv6 environments Secure mobile IPv6 networks Secure transition mechanisms in use during the migration from IPv4 to IPv6 Monitor IPv6 security Understand the security implications of the IPv6 protocol, including issues related to ICMPv6 and the IPv6 header structure Protect your network against large-scale threats by using perimeter filtering techniques and service providerfocused security practices Understand the vulnerabilities that exist on IPv6 access networks and learn solutions for mitigating each This security book is part of the Cisco Press Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks. Category: Networking: Security Covers: IPv6 Security

Learn why IPv6 security matters to your organization, the potential consequences of failing to take prompt action, and the blueprint you need to begin A dual-stack network is as secure as its weakest protocol family. This is called fate-sharing for example, if the IPv6 access is not protected while the IPv4 is controlled, then the malicious user will use IPv6 for the attacks. It is really important to have congruent security policies for IPv4 and IPv6. - 4 min - Uploaded by infosecgovhkIPv6 is a standard protocol for the Internet. To know more about its security features and Why IPv6 Matters for Your Security. Internet Protocol (IP) is the system that allows devices to find and connect to each other online. IPv4 was designed in the This weeks myth is interesting because if we werent talking security it wouldnt be a myth. Say what? The phrase 96 more bits, no magic isLearn about IPv6 transition mechanisms, including, dual-stack, translation and tunneling, and why those mechanisms present enterprise IPv6 security issues Here are the top six security risks in IPv6 network security today as voted by gogoNET members, a community of 95000 network professionals.This paper analyzes how actual security threats and different types of attacks affect IPv6 networks. IPv6 specific security issues and issues due to differentThis is not because of the design IPv6 but because of inadequate support in firewalls and because network administrators and security Today we continue with part 2 of the 10 part series on IPv6 Security Myths by debunking one of the myths I overhear people propagating outThis chapter from Security in an IPv6 Environment by Jake Kouns and Daniel Minoli covers the topics of flows, ICMPv6, neighbor discovery, routing headers, andIPv6 and IPv4 usually operate completely independently over the same Layer 2 infrastructure, so additional and separate IPv6 security mechanisms must beFind out how to work around the implementation-specific IPv6 security challenges that will surface until equipment vendors close the gaps between their IPv4 Most security incidents are down to human error and the lack of experience and training for IT professionals dealing with IPv6 make those Now that were out of IPv4 allocations, its time to get serious about adopting the next generation of Internet Protocol, IPv6.IPv4 network addresses are running out and the deployment of IPv6 This paper considers some of the security concerns for WLCG in an IPv6 world andThis IPv6 tutorial will make understanding IPv6 a bit easier by highlighting IPv6 security issues and discussing IPv6 security threats and features.Learn about the potential hazards of migrating to IPv6 and how to ensure a smooth transition without jeopardizing your companys security.