PowerPackage IPv6

Adressierung, Routing, Interworking, Security

Dieses PowerPackage kombiniert die Inhalte der Kurse IPv6 und IPv6 und Security in einer Veranstaltung.

Die IPv6-Einführung in einem Unternehmensnetzwerk ist sehr facettenreich. Sie setzt ein detailliertes Verständnis der Änderungen und Neuerungen gegenüber IPv4 voraus. Aufbauend auf diesem Wissen kann eine Planung und Umsetzung der Migration erfolgen. Dabei sollten stets auch Sicherheitsaspekte bedacht

Von der Funktionsweise des IPv6-Protokolls über Security-Aspekte bis hin zu sinnvollen Migrationsstrategien erfahren Sie in diesem BootCamp alles, was Sie zum erfolgreichen Einsatz dieser Technologie wissen müssen. Mit diesem Wissen werden Sie in die Lage versetzt, eine strukturierte und sicher durchdachte Migration zu IPv6 zu realisieren.

Kursinhalt

- Die Neuerungen in IPv6
- IPv6 Header, Extension Header und der Aufbau von IPV6-Adressen
- Die IPv6-Kommunikation und deren Schwächen
- Stateless und Stateful Autoconfiguration
- Planung der sicheren Migration von IPv4 auf IPv6
- IPv6 in Endgeräten, Routern und Firewalls
- Tunneln von IPv6 über IPv4
- Interworking von IPv6 mit IPv4 (NAT64 und DNS64)
- Routing und Netzwerkdienste (DNS, DHCP, RADIUS und SNMP) mit IPv6
- Applikationen: WWW, FTP und E-Mail mit IPv6
- Internet Access und ISP-Netze mit IPv6
- Enterprise-Netze und IPv6
- IPv6 in der Mobilfunkwelt
- Security und IPv6: Neue Angriffspunkte, Absicherung, Firewall und VPN

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket aus der Reihe ExperTeach Networking - Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

Zielgruppe

Der Kurs eignet sich für Planer, Administratoren und Security-Beauftragte, die eine Einführung von IPv6 in einem Netzwerk durchführen sollen und mögliche Sicherheitsprobleme bereits im Vorfeld abschätzen wollen.

Voraussetzungen

Detaillierte Kenntnisse zu IPv4 sind für die erfolgreiche Teilnahme notwendig. Eine gute Vorbereitung ist der Besuch des Kurses TCP/IP.

Stand 23.04.2024

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Best finden Sie unter dem folgende www.experteach.ch/go/IP6B und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link:

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

| Training | Preise zzgl. MwSt. | | | | |
|--|---------------------------------|--|--|--|--|
| Termine in Deutschland | 5 TageCHF 2.635,- | | | | |
| Termine in Österreich | 5 TageCHF 2.635,- | | | | |
| Termine in der Schweiz 5 TageCHF 3.150,- | | | | | |
| Online Training 5 TageCHF 2.635,- | | | | | |
| Termin/Kursort | Kurssprache Deutsch | | | | |
| 08.0712.07.24 WMünchen | 21.1025.10.24 WOnline | | | | |
| 08.0712.07.24 WOnline | 21.1025.10.24 Zürich | | | | |
| 16.0920.09.24 Berlin | 18.1122.11.24 Düsseldorf | | | | |
| 16.0920.09.24 WHamburg | 18.1122.11.24 ™ Online | | | | |
| 16.0920.09.24 WOnline | 16.1220.12.24 WOnline | | | | |
| 21.1025.10.24 Frankfurt | 16.1220.12.24 Wien | | | | |



Inhaltsverzeichnis

PowerPackage IPv6 - Adressierung, Routing, Interworking, Security

| | Makada Calo | 4 | DUCD C. Marketon | | Charles to the Control of the Contro |
|---|---|--|--|--|--|
| 1 | Motivation für IPv6 | 5.7.1 | DHCPv6 – Varianten | 8.4.3 | Sicherheitsrelevanz der Erweiterungsheader |
| 1.1 | Die Motivation für IPv6 | 5.7.2 | Stateless DHCPv6 | 8.4.4 | Die Filterung von IPv6 |
| 1.2 | Entwicklungen im Internet | 5.7.3 | Stateful DHCPv6 | 8.5 | Die Sicherheit testen - Tools für IPv6 Vulnerability Tests |
| 1.2.1 | IPv4 Adressraum | 5.7.4 | Lifetime und Erneuerung von Adressen | 8.5.1 | NMAP |
| 1.2.2 | Größe der Routingtabellen | 5.7.5 | DHCPv6-Timing – ohne Server | 8.5.2 | Nessus und OpenVAS |
| 1.2.3 | Effizienz | 5.7.6 | DHCPv6 – Client- und Server-Identifier (DUID) | 8.5.3 | Paket-Generatoren |
| 1.2.4 | Komplexität durch Hilfsprotokolle | 5.8 | DHCPv6 Relay Agent | 8.5.4 | Die THC Toolsammlung |
| 1.3 | Mobilfunk | 5.9 | DHCPv6 Prefix Delegation | 8.5.5 | SI6 Tools |
| 1.3.1 | Mobiles Internet | 5.10 | Die richtige Adressvergabe wählen | | |
| 1.4 | Das Internet of Things (IoT) | 5.11 | IPv6 Adressdesign | 9 | IPv6-Adressierung aus Sicherheitssicht |
| 1.4.1 | IoT Zugangs-Technologien | 5.11.1 | IPv6 Plan für ein Campus Netzwerk | 9.1 | Sicherheitsrelevanz von NAT |
| 1.5 | Anforderungen an das neue IP | 5.11.2 | Adresskonzept VLAN Benennung | 9.1.1 | IPv6-IPv6 Network Prefix Translation (NAT66) |
| 1.6 | Vergleich IPv4 und IPv6 | | | 9.2 | Sicherheitsbetrachtungen zu den Adressarten |
| 1.7 | Die IPv6 Einführung | 6 | IPv6 im Betrieb | 9.2.1 | EUI 64 – Großer Wiedererkennungswert |
| 1.7.1 | Die Einführung in Enterprise-Netzen | 6.1 | Parallelbetrieb IPv6 und IPv4 | 9.2.2 | Temporäre Adressen |
| 1.7.2 | Der Mehrwert für Firmennetze | 6.1.1 | Vor- und Nachteile von Dual Stack | 9.3 | IPv6-Adressen auskundschaften |
| 1.7.3 | Widerstand gegen IPv6 | 6.1.2 | DNS machts möglich | 9.3.1 | Passive Sniffing |
| | | 6.1.3 | Was wird bevorzugt? | 9.3.2 | Detect-New-IP6 |
| 2 | Adressierung mit IPv6 | 6.1.4 | Happy Eyeballs | 9.3.3 | Multicast Enumeration |
| 2.1 | IPv6 Adressen | 6.2 | Betriebssysteme und IPv6 | 9.3.4 | Alive6 |
| 2.2 | Struktur einer IPv6 Adresse | 6.2.1 | Microsoft | 9.3.5 | Registrierungs-Abfrage |
| 2.2.1 | Bilden der Interface ID | 6.2.2 | Linux | 9.3.6 | IPv6 Netze scannen |
| 2.2.2 | Privacy Extensions nach RFC 4941 | 6.2.3 | Mac OS X | 9.3.7 | IPv6-Adressen erraten |
| 2.3 | IPv6 Gültigkeitsbereiche | 6.2.4 | Android | 9.3.8 | DNS Reconnaissance |
| 2.4 | Unicast Adressen | 6.2.5 | iOS | | |
| 2.5 | Global Unicast Adressen | 6.3 | Router und IPv6 | 10 | IPv6 und First Hop Security |
| 2.6 | Link Local Adressen | 6.3.1 | Hersteller | 10.1 | Neighbor-Discovery-Angriffe |
| 2.7 | Unique Local Adressen | 6.3.2 | Cisco Systems | 10.1.1 | Trust Models and Threats |
| 2.7.1 | Vor und Nachteile privater Adressen | 6.3.3 | Juniper | 10.1.2 | NDP Spoofing |
| 2.8 | Multicast Adressen | 6.4 | IPv6 und Virtualisierung | 10.1.3 | Neighbor Unreachability Detection (NUD) |
| 2.8.1 | Bekannte Multicast Adressen | 6.5 | Cloud Services | 10.1.4 | DoS_New_IP6 |
| 2.8.2 | Solicited-Node Multicast Adresse | 6.6 | Routingprotokolle IPv6 | 10.1.5 | NDP Exhaustion Attack |
| 2.8.3 | Präfix basierte Multicast Adressen | 6.6.1 | Statische Routen | 10.1.6 | Neighbor Advertisement Flooding |
| 2.9 | Anycast Adressen | 6.6.2 | RIPng | 10.2 | SLAAC Angriffe |
| 2.10 | Weitere Adresstypen | 6.6.3 | OSPF und IS-IS | 10.2.1 | Rogue Router |
| 2.11 | Die Vergabe der IPv6 Präfixe | 6.6.4 | BGP-4 | 10.2.2 | Man in the Middle mit RAs |
| 2.11.1 | Adressvergabe IANA-RIR | 6.7 | IPv6 beim Zugang | 10.2.3 | Faked Default Gateway |
| 2.11.2 | Adressvergabe der RIRs – LIRs – Kunden | 6.7.1 | IPv6 und PPP | 10.2.4 | RA Flooding |
| 2.11.3 | Kontrolle | 6.7.2 | Konfiguration der WAN-Seite | 10.3 | DHCPv6 Angriffe |
| | | 6.7.3 | Konfiguration der LAN-Seite | 10.3.1 | DHCPv6 Starvation |
| 3 | Der IPv6 – Header | 6.7.4 | Adressierung interner Links | 10.3.2 | Rogue DHCPv6 Server |
| 3.1 | Das Header-Format | | _ | 10.4 | ICMPv6-Angriffe |
| 3.1.1 | Version, Payload Length und Hop Limit | 7 | Die Migration im Überblick | 10.4.1 | Amplification Attack |
| 3.1.2 | Traffic Class | 7.1 | Migrationsverfahren | 10.4.2 | Redirect-Angriffe |
| 3.2 | Flow Label | 7.1.1 | Netze mit Dual Stack Nodes | 10.5 | ACLs zur Sicherung |
| 3.2.1 | RFC 6294: Route Caching und Load Sharing | 7.1.2 | Native IPv6-Netze | 10.5.1 | Rogue Router ausgrenzen |
| 3.2.2 | RFC 6294: Weitere Nutzung des Flow Labels | 7.2 | Tunnel | 10.5.2 | Rogue DHCP Server verhindern |
| 3.3 | Erweiterungen mit dem Next Header | 7.2.1 | IPv6 in IPv4 Tunneling | 10.5.3 | RA Guard |
| 3.3.1 | Erweiterungen für die Router | 7.2.2 | Statische Tunnel – 6in4 | 10.5.4 | DHCPv6 Guard/Shield |
| 3.3.2 | Erweiterungen für die Endsysteme | 7.2.3 | | 10.5.5 | NDP Snooping |
| 3.3.3 | | | Tunnel bauen | | |
| | Erweiterung IPsec | 7.2.4 | Routing durch Tunnel | 10.5.6 | NDP Inspection |
| 3.4 | Erweiterung IPsec Mobile IPv6 | 7.2.4 7.2.5 | Routing durch Tunnel IPv6 in GRE | 10.5.6 10.6 | NDP Inspection SEND |
| 3.4 3.4.1 | Erweiterung IPsec | 7.2.4 7.2.5 7.2.6 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 | 10.5.6 10.6 10.6.1 | NDP Inspection SEND RAS mit SEND absichern |
| 3.4.1 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe | 7.2.4 7.2.5 7.2.6 7.2.7 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 | 10.5.6 10.6 | NDP Inspection SEND |
| 3.4.1 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien | 10.5.6 10.6 10.6.1 10.6.2 | NDP Inspection SEND RAs mit SEND absichern SEND und Stateful Autoconfiguration |
| 3.4.1 4 4.1 | Erweiterung IPsec Mobilie IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First | 10.5.6 10.6 10.6.1 10.6.2 | NDP Inspection SEND RAS mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen |
| 3.4.1 4 4.1 4.2 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 ICMPv6 Meldungen | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First | 10.5.6 10.6 10.6.1 10.6.2 11 11.1 | NDP Inspection SEND RAS mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern |
| 3.4.1 4 4.1 4.2 4.2.1 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen | 10.5.6 10.6 10.6.1 10.6.2 11 11.1 11.1.1 | NDP Inspection SEND RAs mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backtone First Edges First Die Migration planen Das Ziel festlegen | 10.5.6 10.6 10.6.1 10.6.2 11 11.1 11.1.1 11.1.1 | NDP Inspection SEND RAs mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Machbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen | 10.5.6 10.6.1 10.6.2 11 11.1 11.1.1 11.1.2 11.1.3 | NDP Inspection SEND RAS mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Adressen Filtern |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Inventarisierung und Auswertung | 10.5.6 10.6 10.6.1 10.6.2 11 11.1 11.1.1 11.1.2 11.1.3 11.1.4 | NDP Inspection SEND SEND RAS mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLS aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung | 10.5.6 10.6 10.6.1 10.6.2 11 11.1 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 | NDP Inspection SEND RAS mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Adressen Filtern LicMPv6 filtern Sicherung der Routingprotokolle |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Discovery | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests | 10.5.6 10.6.1 10.6.2 11 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 | NDP Inspection SEND SEND RAS mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verker Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.4 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Discovery Neighbor Unreachability Detection | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung | 10.5.6 10.6.1 10.6.2 11 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 | NDP Inspection SEND SEND RAS mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLS aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.4 4.5 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Discovery Neighbor Discovery Neighbor Unreachability Detection Duplicate Address Detection | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? | 10.5.6 10.6.1 10.6.2 11 11.1 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 | NDP Inspection SEND RAS mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Addressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts IP Spoofing verhindern |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.4 4.5 4.6 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Etch Request und Reply Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Router Discovery | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 7.5 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen | 10.5.6 10.6.1 10.6.2 11 11.1 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.1.8 | NDP Inspection SEND SEND RAS mit SEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLS aufsetzen Eingehender Verker Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.4 4.5 4.6 4.7 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Discovery Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Multicast Listener Discovery | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 7.5 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen | 10.5.6 10.6.1 10.6.2 11 11.1 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.1.8 11.2 11.2.1 | NDP Inspection SEND SEND SEND INSEND absichern SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen IPv6-Fähigkeit hinterfragen |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.4 4.5 4.6 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Etch Request und Reply Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Router Discovery | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 7.5 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Zeil festlegen Investratiserung und Auswertung Eine IIPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmaßnahmen | 10.5.6 10.6.1 10.6.2 11 11.1 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.1.8 11.2 11.2.1 | NDP Inspection SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen IPv6-Fahigkeit hinterfragen Check Point |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.3 4.4 4.5 4.6 4.7 4.8 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Multicast Listener Discovery Redirect | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 7.5 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmaßnahmen Personal und Dienstleister | 10.5.6 10.6.1 10.6.2 11 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.1.8 11.2.1 11.2.1 | NDP Inspection SEND SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4- Verwendung von Link Local Unicasts IPv5-Pahigkeit hinterfragen Check Point Cisco-ASA |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.4 4.5 4.6 4.7 4.8 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Discovery Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Multicast Listener Discovery Redirect Adressvergabe mit IPv6 | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 7.5 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarsierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmaßnahmen Personal und Dienstleister IPv4 und IPv6 – Sicherheit im Vergleich | 10.5.6 10.6.1 10.6.2 11 11.1 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.1.8 11.2 11.2.1 11.2.1 11.2.2 | NDP Inspection SEND SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen IPv6-Fähigkeit hinterfragen Check Point Cisco-ASA Palo Alto |
| 3.4.1 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.4 4.5 4.6 4.7 4.8 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 12: Exceeded Typ 4: Parameter Problem Typ 12: Exche Request und Reply Neighbor Discovery Neighbor Discovery Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Multicast Listener Discovery Redirect Adressvergabe mit IPv6 Adressvergabe bei IPv6 | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 7.5 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmaßnahmen Personal und Dienstleister IPv4 und IPv6 – Sicherheit im Vergleich Unterschiede zwischen IPv4 und IPv6 | 10.5.6 10.6.1 10.6.2 11 11.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.1.8 11.2 11.2.1 11.2.2 11.2.1 11.2.2 11.2.3 11.2.4 11.2.5 | NDP Inspection SEND SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen IPv6-Fähigkeit hinterfragen Check Point Cisco-ASA Palo Alto Fortinet |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.4 4.5 4.3 4.4 4.5 5.1 5.2 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Discovery Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Multicast Listener Discovery Redirect Adressvergabe mit IPv6 Adressvergabe bei IPv6 Statische Adressvergabe | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.3.2 7.4 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 7.5 8 8.1 8.1.1 8.1.1 8.1.2 8.2 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmaßnahmen Personal und Dienstleister IPv4 und IPv6 – Sicherheit im Vergleich Unterschiede zwischen IPv4 und IPv6 Die aktuelle Sicherheitslage | 10.5.6 10.6.1 10.6.2 11 11.1.1 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.1.8 11.2.1 11.2.1 11.2.2 11.2.3 11.2.4 11.2.5 11.2.5 | NDP Inspection SEND SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLS aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 - Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen IPv6-Fähigkeit hinterfragen Check Point Cisco-ASA Palo Alto Fortniet Juniper |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.3 4.2.4 4.2.5 4.3 4.4 4.5 4.6 4.7 4.8 5 5.1 5.2 5.3 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Discovery Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Multicast Listener Discovery Multicast Listener Discovery Redirect Adressvergabe bei IPv6 Statische Addressvergabe Router Addrestiements deaktivieren? | 7.2.4 7.2.5 7.2.6 7.2.7 7.3.1 7.3.1 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 8.8.1 8.1.1 8.1.2 8.2.1 8.3.3 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarsierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmaßnahmen Personal und Dienstleister IPv4 und IPv6 – Sicherheit im Vergleich Unterschiede zwischen IPv4 und IPv6 Die aktuelle Sicherheitslage Vulnerable IPv6 Stacks | 10.5.6 10.6.1 10.6.2 11 11.1 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.2 11.2.1 11.2.2 11.2.3 11.2.4 11.2.4 11.2.5 11.2.6 | NDP Inspection SEND SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen IPv6-Fähigkeit hinterfragen Check Point Cisco-ASA Palo Alto Fortinet Juniper Barracuda |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.4 4.5 5 5.1 5.2 5.3 5.4 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 1: Sp12: Echo Request und Reply Neighbor Discovery Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Multicast Listener Discovery Multicast Listener Discovery Redirect Adressvergabe mit IPv6 Statische Adressvergabe Router Addressvergabe | 7.2.4 7.2.5 7.2.6 7.2.7 7.3.1 7.3.1 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 8 8.1 8.1.1 8.1.2 8.2 8.2.1 8.3.1 8.3.1 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundstatliche Überlegungen Sicherheitsmaßnahmen Personal und Dienstleister IPv4 und IPv6 – Sicherheit im Vergleich Unterschiede zwischen IPv4 und IPv6 Die aktuelle Sicherheitslage Vulnerable IPv6 Stacks Die Firewall | 10.5.6 10.6.1 10.6.1 11.1 11.1 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.1.8 11.2 11.2.1 11.2.1 11.2.1 11.2.1 11.2.1 11.2.1 11.2.1 11.2.1 11.2.1 | NDP Inspection SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLS aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen IPv6-Fähigkeit hinterfragen Check Point Cisco-ASA Palo Alto Fortinet Juniper Barracuda Objekte anpassen |
| 3.4.1 4 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.4 4.5 5.6 5.1 5.2 5.3 5.4 5.5 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Discovery Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Multicast Listener Discovery Redirect Adressvergabe mit IPv6 Adressvergabe bei IPv6 Statische Advertisements deaktivieren? Dynamische Adressvergabe Stateless Autoconfiguration (SLAAC) | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.4.1 7.4.2 7.4.3 7.4.5 7.5 8 8.1 8.1.1 8.1.2 8.2 8.2.1 8.3 8.3.1 8.3.2 8.3.3 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmäßnahmen Personal und Dienstleister IPv4 und IPv6 – Sicherheit im Vergleich Unterschiede zwischen IPv4 und IPv6 Die aktuelle Sicherheitslage Vulnerable IPv6 Stacks Die Firewall Intrusion Prevention System | 10.5.6 10.6.1 10.6.2 11 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.1.8 11.2.1 11.2.2 11.2.1 11.2.2 11.2.3 11.2.4 11.2.5 11.2.6 11.2.7 | NDP Inspection SEND SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLS aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 - Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen IPv6-Fähigkeit hinterfragen Check Point Cisco-ASA Palo Alto Fortinet Juniper Barracuda Objekte anpassen Regelwerke ergänzen |
| 3.4.1 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.3 4.4 5 4.6 4.7 4.8 5 5.1 5.2 5.3 5.4 5.5 5.5 5.5 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Discovery Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Multicast Listener Discovery Multicast Listener Discovery Redirect Adressvergabe mit IPv6 Adressvergabe bei IPv6 Statische Addressvergabe Router Advertisements deaktivieren? Dynamische Addressvergabe Stateless Autoconfiguration (SLAAC) Prozesse während SLAAC | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.4.1 7.4.2 7.4.3 7.4.5 7.5 8 8.1 8.1.1 8.1.2 8.2 8.3 8.3.1 8.3.1 8.3.2 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmaßnahmen Personal und Dienstleister IPv4 und IPv6 – Sicherheit im Vergleich Unterschiede zwischen IPv4 und IPv6 Die aktuelle Sicherheitslage Vulnerable IPv6 Stacks Die Firewall Intrusion Prevention System Der IPv6-Header aus Sicherheitssicht | 10.5.6 10.6.1 10.6.1 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.2.1 11.2.1 11.2.2 11.2.3 11.2.4 11.2.5 11.2.6 11.2.7 11.2.8 | NDP Inspection SEND SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 - Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen IPv6-Fähigkeit hinterfragen Check Point Cisco-ASA Palo Alto Fortinet Juniper Barracuda Objekte anpassen Regelwerke ergänzen Bogon Filtering |
| 3.4.1 4 4.1 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.5 4.6 4.7 4.8 5 5.1 5.2 5.3 5.4 5.5 5.5.1 5.6 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 1: Stoscovery Neighbor Discovery Neighbor Discovery Neighbor Discovery Multicast Listener Discovery Multicast Listener Discovery Multicast Listener Discovery Redirect Adressvergabe mit IPv6 Adressvergabe bei IPv6 Statische Addressvergabe Stateless Autoconfiguration (SLAAC) Prozesse während SLAAC IPv6 RDNSS Configuration | 7.2.4 7.2.5 7.2.7 7.3 7.3.1 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 8.1 8.1.1 8.1.1 8.2 8.2 8.2 8.3 8.3 8.3 8.3 8.4 8.4 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmaßnahmen Personal und Dienstleister IPv4 und IPv6 – Sicherheit im Vergleich Unterschiede zwischen IPv4 und IPv6 Die aktuelle Sicherheitslage Vulnerable IPv6 Stacks Die Firewall Intrusion Prevention System Der IPv6-Header aus Sicherheitssicht Das Flow Label – Covert Channel | 10.5.6 10.6.1 10.6.2 11 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.2.1 11.2.1 11.2.1 11.2.2 11.2.3 11.2.4 11.2.5 11.2.4 11.2.5 11.2.4 11.2.5 11.2.1 11.2.4 11.2.5 11.2.1 11.2.4 11.2.5 11.2.1 11.2.4 11.2.5 11.2.1 | NDP Inspection SEND SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLS aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts IP Spoofing verhindern IPv6-Fähigkeit hinterfragen Check Point Cisco-ASA Palo Alto Fortinet Juniper Barracuda Objekte anpassen Regelwerke ergänzen Bogon Filtering Radius und IPv6 |
| 3.4.1 4.1 4.2 4.2.1 4.2.2 4.2.3 4.2.4 4.3 4.4 5 4.6 4.7 4.8 5 5.1 5.2 5.3 5.4 5.5 5.5 5.5 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 128/129: Echo Request und Reply Neighbor Discovery Neighbor Unreachability Detection Duplicate Address Detection Router Discovery Multicast Listener Discovery Multicast Listener Discovery Redirect Adressvergabe mit IPv6 Adressvergabe bei IPv6 Statische Addressvergabe Router Advertisements deaktivieren? Dynamische Addressvergabe Stateless Autoconfiguration (SLAAC) Prozesse während SLAAC | 7.2.4 7.2.5 7.2.6 7.2.7 7.3 7.3.1 7.4.1 7.4.2 7.4.3 7.4.5 7.5 8 8.1 8.1.1 8.1.2 8.2 8.3 8.3.1 8.3.1 8.3.2 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmaßnahmen Personal und Dienstleister IPv4 und IPv6 – Sicherheit im Vergleich Unterschiede zwischen IPv4 und IPv6 Die aktuelle Sicherheitslage Vulnerable IPv6 Stacks Die Firewall Intrusion Prevention System Der IPv6-Header aus Sicherheitssicht | 10.5.6 10.6.1 10.6.2 11 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.2.1 11.2.1 11.2.1 11.2.2 11.2.3 11.2.4 11.2.5 11.2.4 11.2.5 11.2.4 11.2.5 11.2.1 11.2.4 11.2.5 11.2.1 11.2.4 11.2.5 11.2.1 11.2.4 11.2.5 11.2.1 | NDP Inspection SEND SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLs aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 - Verwendung von Link Local Unicasts IP Spoofing verhindern Firewalls anpassen IPv6-Fähigkeit hinterfragen Check Point Cisco-ASA Palo Alto Fortinet Juniper Barracuda Objekte anpassen Regelwerke ergänzen Bogon Filtering |
| 3.4.1 4 4.1 4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.5 4.6 4.7 4.8 5 5.1 5.2 5.3 5.4 5.5 5.5.1 5.6 | Erweiterung IPsec Mobile IPv6 Mobile IPv6 Begriffe Nachbarschaftsprozesse ICMPv6 ICMPv6 Meldungen Typ 1: Destination Unreachable Typ 2: Packet to Big Typ 3: Time Exceeded Typ 4: Parameter Problem Typ 1: Stoscovery Neighbor Discovery Neighbor Discovery Neighbor Discovery Multicast Listener Discovery Multicast Listener Discovery Multicast Listener Discovery Redirect Adressvergabe mit IPv6 Adressvergabe bei IPv6 Statische Addressvergabe Stateless Autoconfiguration (SLAAC) Prozesse während SLAAC IPv6 RDNSS Configuration | 7.2.4 7.2.5 7.2.7 7.3 7.3.1 7.4.1 7.4.2 7.4.3 7.4.4 7.4.5 8.1 8.1.1 8.1.1 8.2 8.2 8.2 8.3 8.3 8.3 8.3 8.4 8.4 | Routing durch Tunnel IPv6 in GRE Dynamische Tunnel – 6to4 Adressformat bei 6to4 Migrationsstrategien Backbone First Edges First Edges First Die Migration planen Das Ziel festlegen Den Ist-Zustand erfassen Inventarisierung und Auswertung Eine IPv6-Testumgebung Abschluss der Tests Umstellen – Aber wann? Grundlegende Sicherheitsüberlegungen Grundsätzliche Überlegungen Sicherheitsmaßnahmen Personal und Dienstleister IPv4 und IPv6 – Sicherheit im Vergleich Unterschiede zwischen IPv4 und IPv6 Die aktuelle Sicherheitslage Vulnerable IPv6 Stacks Die Firewall Intrusion Prevention System Der IPv6-Header aus Sicherheitssicht Das Flow Label – Covert Channel | 10.5.6 10.6.1 10.6.2 11 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.1.7 11.2.1 11.2.1 11.2.1 11.2.2 11.2.3 11.2.4 11.2.5 11.2.4 11.2.5 11.2.4 11.2.5 11.2.1 11.2.4 11.2.5 11.2.1 11.2.4 11.2.5 11.2.1 11.2.4 11.2.5 11.2.1 | NDP Inspection SEND SEND SEND SEND und Stateful Autoconfiguration Sicherheit von IPv6-Netzen Router in IPv6 Netzwerken sichern IPv6 ACLS aufsetzen Eingehender Verkehr Adressen Filtern ICMPv6 filtern Sicherung der Routingprotokolle Authentisierung bei Routing Protokollen BGP-4 – Verwendung von Link Local Unicasts IP Spoofing verhindern IPv6-Fähigkeit hinterfragen Check Point Cisco-ASA Palo Alto Fortinet Juniper Barracuda Objekte anpassen Regelwerke ergänzen Bogon Filtering Radius und IPv6 |











