GLOBEPEER TECHNICAL SERVICE DESCRIPTION

I. ALLGEMEINE BESTIMMUNGEN

1. Überblick, Geltungsbereich

Dieses Dokument beinhaltet die Technical Service Description (TSD) für den GlobePEER Service. Diese TSD ist Teil des Rahmenvertragswerks.

Diese TSD findet nur Anwendung auf den GlobePEER Service. Der GlobePEER Service kann jedoch Voraussetzung für andere Services sein. Dieses Dokument beinhaltet nur technische Spezifikationen und Dokumentationen. Die Service Level für GlobePEER sind im GlobePEER Special Service Level Agreement (Special SLA) beschrieben.

Für jeden Ruhr-CIX GlobePEER Service, wird ein Ruhr-CIX GlobePEER Remote Service Düsseldorf in der entsprechend gleichen Kapazität ohne zusätzliche Kosten zur Verfügung gestellt und muss konfiguriert werden (siehe Ruhr-CIX AGB).

2. Anpassung

Dieses Dokument kann jederzeit gemäß den Bestimmungen des Ruhr-CIX Agreement überarbeitet und ergänzt werden.

3. Produktvoraussetzungen

Der GlobePEER Service erfordert die folgenden Ruhr-CIX Services für seinen normalen Betrieb:

- Access (siehe Master SLA und Technical Access Description (TAD)) an einem Rechenzentrumsstandort, an dem lokaler oder Remote-Zugang zu der jeweiligen GlobePEER Region angeboten wird.

4. Anwendbare Standards

Die Nutzung des Ruhr-CIX Netzwerks durch den Kunden hat zu jeder Zeit in Übereinstimmung mit den relevanten Standards, wie sie in STD0001 und verbundenen Internet STD Dokumenten niedergelegt sind, zu erfolgen.

II. KONFIGURATION SICHERUNGSSCHICHT (ISO/OSI LAYER 2)

1. Bandbreite

Die Bandbreite des GlobePEER Services muss statisch konfiguriert werden, falls die vereinbarte Bandbreite für GlobePEER sich von der Bandbreite des Zugangs oder des Bündels von zusammengefassten Zugängen unterscheidet, auf dem der GlobePEER Service genutzt wird.

2. Frame Typen

Die folgenden allgemeinen Regeln gelten:

Frame Typ (Ethertype)	**Regel**	**Durchsetzung**
0x0800 – IPv4 0x0806 – ARP 0x86dd – IPv6	**Erlaubt**	-
Alle anderen Typen	**Verwerfen**	Strikt – alle Frames außer den erlaubten Typen werden verworfen

3. MAC Adressen Konfiguration

Alle Frames, die zum GlobePEER Service weitergeleitet werden, müssen dieselbe Ursprungs-MAC-Adresse haben.

4. Broadcast/Multicast Traffic

Die folgenden Regeln gelten für den Broadcast/Multicast Traffic:

Protokoll	Regel	Durchsetzung
Broadcast ARP (außer proxy ARP), multicast IPv6 Neighbor Discovery (ND)	**Erlaubt, aber Durchsatz limitiert auf 1,000kbps**	-
Alle anderen Typen, d.h. einschließlich, aber nicht beschränkt auf: - IRDP - ICMP redirects - IEEE802 Spanning Tree - Herstellerspezifische Discovery Protokolle (z.B. CDP) - Interior routing protocol broad/multicasts (e.g. OSPF, IS-IS, IGRP, EIGRP) - BOOTP/DHCP - PIM-SM - PIM-DM - DVMRP	**Verwerfen**	Werden verworfen, sofern nicht ausdrücklich erlaubt

III. KONFIGURATION VERMITTLUNGSSCHICHT (ISO/OSI LAYER 3)

1. Schnittstellen Konfiguration

Schnittstellen, die mit Ruhr-CIX Ports verbunden sind, dürfen nur IP Adressen und Subnetzmasken (Präfix Längen) nutzen, die ihnen von Ruhr-CIX zugewiesen wurden. Die Zuweisung wird schriftlich (z.B. E-Mail) während des Bereitstellungsprozesses erfolgen. Insbesondere:

DE CIX DOKOM21 GELSEN-NET 100% IT vor Ort TMR Telekommunikation Mittleres Ruhrgebiet www.tmr.net

Parameter	Regel	Bemerkungen
IP Adressen (IPv4, IPv6), inklusive Subnetzmasken für ihre Schnittstellen	**IPv4 erforderlich**	Zumindest die IPv4 Adresse muss konfiguriert werden
IP Adresse von Route Servern	**Erforderlich für Geltendmachung von Credits**	Mindestens eine BGP Sitzung mit einem Route Server muss konfiguriert sein, um Credits für den GlobePEER Service geltend machen zu können. Das Advertising von Routen ist nicht notwendig.

2. Zusätzliche Konfigurations-Parameter

Parameter	Regel	Bemerkungen
IPv6 Adressen (link-lokal & global)	**Keine Auto-Konfiguration**	Alle IPv6 Adressen müssen statisch konfiguriert sein
IPv6 Adresse (site-lokal)	**Nicht erlaubt**	IPv6 site-lokale Adressen dürfen nicht genutzt werden
Standard MTU	**Feste Größe**	Standard IP MTU Größe muss statisch auf 1.500 Bytes gesetzt werden, sofern nicht ausdrücklich schriftlich anders vereinbart

3. Routing Konfiguration

Die Routing-Konfiguration des Kundensystems muss die folgenden Regeln/Einstellungen enthalten:

Parameter	Regel	Bemerkungen
BGP Version	**Nur v. 4**	-
AS Nummern	**Nur öffentliche**	Es sind keine privaten AS Nummern erlaubt.
Mehrere ASN	**Erlaubt**	Kunden dürfen mehr als eine ASN für ihr Peering nutzen, soweit jede verwendete ASN die gleichen NOC- und Peering-Kontaktdaten hat.
Route Advertising	**Größtmögliche Zusammen-fassung**	Alle Routen, die per Advertising bekanntgegeben werden, sind soweit wie möglich zusammenzufassen.
Route Advertising – Ziel IP	**Nur Advertising Router**	Alle Routen, die per Advertising dem Ruhr-CIX Netzwerk bekannt gegeben werden, dürfen als Ziel nur den bekanntgebenden Router nennen, sofern im Voraus keine schriftliche abweichende Vereinbarung mit Ruhr-CIX und den betroffenen Kunden geschlossen wurde.
Route Advertising – Registrierung	**Öffentliche Registrierung erforderlich**	Alle Routen, die im Rahmen einer Peering Sitzung dem Ruhr-CIX Netzwerk bekannt gegeben werden sollen, müssen in der RIPE Datenbank oder einer anderen öffentlichen Datenbank registriert sein.
IP-Adressraum Advertising	**Nur mit Erlaubnis**	IP-Adressraum, der dem Peering LAN zugeordnet ist, darf nicht ohne ausdrückliche Erlaubnis in anderen Netzen bekannt gegeben werden.
Ruhr-CIX Advertised Routes	**Akzeptieren**	Kunden können Routen, die von Ruhr-CIX bekannt gegeben werden, ohne Bedenken akzeptieren, da sämtliche eingehenden Routen gemäß der eingestellten Richtlinien gefiltert werden.

4. Traffic Weiterleitung

Netzwerk Traffic soll nur dann zu einem Ruhr-CIX Kunden weitergeleitet werden, sofern dazu eine Erlaubnis durch den empfangenden Kunden erteilt wurde, entweder:

- durch Bekanntgabe einer Route über das Ruhr-CIX Netzwerk (direkt oder über den Route Server)
- oder ausdrücklich in schriftlicher Form

5. Route Server Funktion

Das Route Server System besteht aus zwei Servern. Für den normalen Betrieb wird nur einer benötigt.

5.1 Mindestkonfiguration

Damit die Messungen der Route Server Funktion funktionieren, und damit ein Kunde Credits geltend machen kann, muss zumindest eine Verbindung zu einem Route Server mit den folgenden Parametern eingerichtet sein:

Parameter	**Regel**	**Bemerkungen**
Verbindungsmodus	**Aktiv**	Ruhr-CIX Seite ist als passiv konfiguriert
bgp enforce-first-as	**Nicht erlaubt**	Standardmäßig aktiviert, muss manuell deaktiviert werden
AS-Set	**Erforderlich**	Ruhr-CIX braucht das AS-Set des Kunden um die Filterregeln zu erstellen
martians/bogons	**Werden verworfen**	

5.2 Validierung von BGP Announcements

BGP Bekanntmachungen, die vom Kunden an den Route Server zur Verfügung gestellt werden, werden aus Sicherheitsgründen geprüft. Es können Datenbanken für die Routen Validierung genutzt werden (z.B. RADB).

5.3 Optional: Communities

Zusätzlich zu der Ein-Route-Server minimal Konfiguration kann der Kunden sich dafür entscheiden, ausgehende Routing Informationen direkt auf den Route Servern zu kontrollieren, indem er Communities (wobei „Communities“ auch „Extended Communities“ in 32-bit AS Umgebungen meint) hinzufügt. Communities werden von den Ruhr-CIX Route Servern anhand des folgenden Satzes von Filter-Regeln verarbeitet:

#	Aktion	Community	Lokale Präferenz
1	Bekanntgabe einer Route an einen bestimmten Peer blockieren	0:<peer-as>	50
2	Bekanntgabe einer Route an einen bestimmten Peer	<route-server-as>:<peer-as>	
3	Bekanntgabe einer Route an alle Peers blockieren (monitoring only session)	0:<route-server-as>, no advertise, no-export	0
4	Bekanntgabe einer Route an alle Peers	<route-server-as>:<route-server-as> (default if nothing set)	100

Die Zahl und Liste der verfügbaren Communities kann zwischen den GlobePEER Regionen und Standorten variieren. Kunden werden gebeten, die standortspezifische Dokumentation der bestehenden Communities, die auf Anfrage verfügbar gemacht wird, zu konsultieren.

6. Blackholing

Blackholing bedeutet den Datenfluss auf einen anderen next Hop (das “Blackhole”) umzuleiten, wo der Traffic verworfen wird. Das Ergebnis ist, dass kein Traffic das Originalziel erreicht und damit Hosts innerhalb der „blackholed“ Präfixe vor massiven Distributed Denial of Sevice (DDoS) Attacken geschützt werden, die die Verbindungen vom Kunden zu Ruhr-CIX überlasten. Damit ist Blackholing ein effektiver Weg um die Effekte von DDoS Attacken zu vermindern.

Ruhr-CIX stellt die technische Infrastruktur zur Verfügung, die es den Kunden erlaubt, Blackholing einzurichten und zu nutzen. Allerdings entzieht es sich der Kontrolle von Ruhr-CIX, ob ein bestimmter Kunde „blackholed“ Präfixe akzeptiert oder nicht.

6.1 Grundprinzip

6.1.1 Im Normalbetrieb

Kunden geben ihre Präfixe mit einer next Hop Adresse an, die zu ihrer AS gehört:

- IPv4: /8 <= und <= /24
- IPv6: /19 <= und <= /48

6.1.2 Im Falle eines DDoS

Kunden geben ihre Präfixe mit einer eindeutigen von Ruhr-CIX bereitgestellten Blackhole next Hop IP-Adresse (BN) an:

- IPv4: /8 <= bis zu = /32 (nur wenn die BN gesetzt ist)
- IPv6: /19 <= bis zu = /128 (nur wenn die BN gesetzt ist)

Die standardmäßige Prüfung von Announcements findet gleichwohl statt.

6.2 L2 Filterung

- Blackhole next Hop (BN) hat eine eindeutige MAC Adresse (bestimmt von ARP für die BN IP Adresse) z.B. de:ad:be:ef:66:95
- ARP/ND Auflösung für die Blackhole IP next hop wird derzeit durch host buoy bereitgestellt.
- Alle edge nodes haben einen statischen Eintrag für die eindeutige MAC Adresse
- Attackierender Traffic wird vom Kunden an den Service mit der statischen MAC Adresse weitergeleitet, und dringt nicht weiter vor. Dies führt dazu, dass der bösartige Traffic die Eingangsnode des GlobePEER Services nicht verlässt, sondern dort lokal verworfen wird.

6.3 Ergebnis

Im Ergebnis wird der gesamte Traffic auf den attackierten und “blackholed” IP Präfix bereits auf dem ankommenden Switch verworfen und damit die Ressourcen des Opfers (z.B. Verbindung vom Kunden zu Ruhr-CIX) geschützt.