

DE-CIX 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 DE-CIX Rahmenvertragswerks.

Diese TSD findet nur Anwendung auf den GlobePEER Service. Der GlobePEER Service kann jedoch Voraussetzung für andere DE-CIX 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.

2. Anpassung

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

3. Produktvoraussetzungen

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

- DE-CIX Access (siehe Master SLA und DE-CIX Technical Access Description (TAD)) an einem Rechenzentrumsstandort, an dem lokaler oder Remote-Zugang¹ zu der jeweiligen GlobePEER Region angeboten wird.

4. Anwendbare Standards

Die Nutzung des DE-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.

¹ Einige Exchange Standorte von DE-CIX sind miteinander verbunden. An diesen Standorten können Kunden Zugang zu der GlobePEER Region am Remote-Standort als zusätzlichen Service buchen, z. B. können Kunden der DE-CIX New York Region den Zugang zur DE-CIX GlobePEER Frankfurt Region bestellen.

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:

<u>Frame Typ (Ethertypen)</u>	<u>Regel</u>	<u>Durchsetzung</u>
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:

<u>Protokoll</u>	<u>Regel</u>	<u>Durchsetzung</u>
Broadcast ARP (außer proxy ARP), multicast IPv6 Neighbor Discovery (ND) (Dies schließt keine Router Advertisement (ND-RA) Pakete ein!)	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 DE-CIX Ports verbunden sind, dürfen nur IP Adressen und Subnetzmasken (Präfix Längen) nutzen, die ihnen von DE-CIX zugewiesen wurden. Die

Zuweisung wird schriftlich (z.B. E-Mail) während des Bereitstellungsprozesses erfolgen.
Insbesondere:

<u>Parameter</u>	<u>Regel</u>	<u>Bemerkungen</u>
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

<u>Parameter</u>	<u>Regel</u>	<u>Bemerkungen</u>
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:

<u>Parameter</u>	<u>Regel</u>	<u>Bemerkungen</u>
BGP Version	Nur v. 4	-
AS Nummern	Nur öffentliche	Es sind keine privaten AS Nummern erlaubt.
Mehrere ASN	Erlaubt	Jeder GlobePEER Service ist durch eine ASN definiert. Wenn ein Kunde mehrere ASNs nutzen möchte, müssen mehrere GlobePEER Services verwendet werden. Jede verwendete ASN muss die gleichen NOC- und Peering-Kontaktdaten haben.
Route Advertising	Größtmögliche Zusammenfassung	Alle Routen, die per Advertising bekannt gegeben werden, sind soweit wie möglich zusammenzufassen.
Route Advertising – Ziel IP	Nur Advertising Router	Alle Routen, die per Advertising dem DE-CIX Netzwerk bekannt gegeben werden, dürfen als Ziel nur den bekanntgebenden Router nennen, sofern im Voraus keine schriftliche abweichende Vereinbarung mit DE-CIX und den betroffenen Kunden geschlossen wurde.
Route Advertising – Registrierung	Öffentliche Registrierung erforderlich	Alle Routen, die im Rahmen einer Peering Sitzung dem DE-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 DE-CIX Peering LAN zugeordnet ist, darf nicht ohne ausdrückliche Erlaubnis in anderen Netzen bekannt gegeben werden.

DE-CIX Advertised Routes	Akzeptieren	Kunden können Routen, die von DE-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 DE-CIX Kunden weitergeleitet werden, sofern dazu eine Erlaubnis durch den empfangenden Kunden erteilt wurde, entweder:

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

5. Route Server Funktion

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

5.1 Mindestkonfiguration

Damit die DE-CIX 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:

<u>Parameter</u>	<u>Regel</u>	<u>Bemerkungen</u>
Verbindungsmodus	Aktiv	DE-CIX Seite ist als passiv konfiguriert
bgp enforce-first-as	Nicht erlaubt	Standardmäßig aktiviert, muss manuell deaktiviert werden
AS-Set	Erforderlich	DE-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 DE-CIX 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 DE-CIX Route Servern zu kontrollieren, indem er Communities (wobei „Communities“ auch „Extended Communities“ in 32-bit AS Umgebungen meint) hinzufügt. Communities werden von den DE-CIX Route Servern anhand des folgenden Satzes von Filter-Regeln verarbeitet:

#	<u>Aktion</u>	<u>Community</u>	<u>Lokale Präferenz</u>
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 Service (DDoS) Attacken geschützt werden, die die Verbindungen vom Kunden zu DE-CIX überlasten. Damit ist Blackholing ein effektiver Weg um die Effekte von DDoS Attacken zu vermindern.

DE-CIX stellt die technische Infrastruktur zur Verfügung, die es den Kunden erlaubt, Blackholing einzurichten und zu nutzen. Allerdings entzieht es sich der Kontrolle von DE-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 DE-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 Eingangsnodes 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 DE-CIX) geschützt.