DebTik Network Appliance

Επίσημος Οδηγός Routing Filters, BGP Policies & Traffic Engineering

Έκδοση Λογισμικού: 1.3.11+ | Routing Engine: BIRD 2 (v2.17+) | Σύνταξη: MikroTik RouterOS v7 Scripting Layer | Ημερομηνία: Νοέμβριος 2026

1. Εισαγωγή & Αρχιτεκτονική Λειτουργίας

Τα Routing Filters στο DebTik αποτελούν τον πυρήνα επιβολής πολιτικής δρομολόγησης (Routing Policy) για τη διαχείριση διαδρομών στα πρωτόκολλα BGP και OSPF. Η υλοποίηση βασίζεται στην πανίσχυρη μηχανή δρομολόγησης BIRD 2, παρέχοντας ταυτόχρονα ένα συντακτικό επίπεδο απόλυτα συμβατό με το γνώριμο περιβάλλον του MikroTik RouterOS v7.

Ο μηχανισμός λειτουργεί με τις εξής θεμελιώδεις αρχές:

- Αλυσίδες Κανόνων (Chains): Οι κανόνες ομαδοποιούνται σε λογικές αλυσίδες (π.χ. Internal, bgp-in, bgp-out). Κάθε αλυσίδα μεταφράζεται στο BIRD 2 σε διαδικαστική συνάρτηση function fn_filter_<Chain>() και σε αυτόνομο φίλτρο filter filter_<Chain>.
- Σειριακή Εκτέλεση (Rule Order): Οι κανόνες αξιολογούνται αυστηρά με βάση τον αριθμό σειράς (#, π.χ. 10, 20, 30). Ο μικρότερος αριθμός προηγείται.
- Τερματικές Ενέργειες (Terminal Actions): Το accept; ή το reject; τερματίζει ακαριαία την αξιολόγηση της αλυσίδας για τη συγκεκριμένη διαδρομή. Το αποτέλεσμα εφαρμόζεται άμεσα.
- Μη-τερματική Επεξεργασία (Passthrough): Επιτρέπει την τροποποίηση ιδιοτήτων (Local Preference, Communities, Prepending, Metric) χωρίς διακοπή της αλυσίδας, επιτρέποντας στη διαδρομή να ελεγχθεί από επόμενους κανόνες.
- Πολιτική Προεπιλεγμένης Απόρριψης (Default Deny): Αν μια διαδρομή περάσει όλους τους κανόνες μιας αλυσίδας χωρίς να ταιριάξει σε κανέναν (unmatched), απορρίπτεται αυτόματα στο τέλος (reject;).

ΑΥΤΟΜΑΤΗ ΠΡΟΣΤΑΣΙΑ: Αρχιτεκτονική Προστασία Έκδοσης 1.3.11+: Στα εξερχόμενα φίλτρα BGP (OutFilter), το DebTik εξασφαλίζει ότι τα ρητά δηλωμένα Advertised Networks (Output Networks / Static Blackhole) και οι επιλογές αναδιανομής (Connected/Static) προστατεύονται αυτόματα και δεν απορρίπτονται από το default reject, εκτός αν υπάρχει ρητός κανόνας απόρριψης από τον χρήστη.

Επισκόπηση Κύριων Δυνατοτήτων DebTik Routing Engine:

Λειτουργική Δυνατότητα	Περιγραφή & Τεχνική Υλοποίηση
v7 Procedural Scripting	Σύνταξη if (συνθήκη) { ενέργειες; } με πλήρη υποστήριξη λογικών τελεστών (&&, ||, !).
CIDR & Subnet Ranges	Αντιστοίχιση υποδικτύων με εύρος μάσκας (π.χ. dst in 10.0.0.0/8{24,28}) ή ακριβές μήκος μάσκας (net.len = 24).
BGP Traffic Engineering	Πλήρης έλεγχος διαδρομών με BGP Local Preference, MED Metric, AS-Path Prepending και Community manipulation.
Named Lists	Επαναχρησιμοποιήσιμες ονομαστικές λίστες Community Lists και AS-Path Lists για απλοποίηση κανόνων.
Visual Rule Wizard	Ενσωματωμένος γραφικός οδηγός δημιουργίας κανόνων με έτοιμα Quick Templates για άμεση εισαγωγή.

2. Δομή Διεπαφής Χρήστη & Διαχείριση (Web UI)

Η διαχείριση των Routing Filters γίνεται από το Web Interface στη διαδρομή Routing → Policy Filters. Η οθόνη περιλαμβάνει 3 λειτουργικές καρτέλες, κεντρική εργαλειοθήκη (Toolbar) και παράθυρα διαμόρφωσης (Modals):

Καρτέλα (Tab)	RouterOS Path	Περιγραφή & Λειτουργία στο BIRD 2
Rules	`/routing filter rule`	Εκτελέσιμοι κανόνες φιλτραρίσματος. Ορίζουν κριτήρια ελέγχου και ενέργειες (Accept/Reject/Set). Μεταφράζονται σε BIRD 2 filters.
Community Lists	`/routing filter community-list`	Ονομαστικές λίστες BGP Communities (π.χ. 65000:100). Μεταφράζονται σε define comm_<Name> = [...].
AS Lists	`/routing filter num-list`	Ονομαστικές λίστες αυτόνομων συστημάτων (ASNs / Ranges). Μεταφράζονται σε define aslist_<Name> = [...].

2.1 Εργαλεία Toolbar

- + New: Άνοιγμα του modal δημιουργίας νέου στοιχείου ανάλογα με την ενεργή καρτέλα.
- Enable / Disable: Άμεση ενεργοποίηση ή απενεργοποίηση της επιλεγμένης γραμμής. Η κατάσταση επισημαίνεται με σημαία A (Active - Κυανό) ή X (Disabled - Κόκκινο).
- Remove: Οριστική διαγραφή του επιλεγμένου κανόνα ή λίστας.
- Chain Filter Dropdown: Επιλογή συγκεκριμένης αλυσίδας (π.χ. Internal) για εστιασμένη προβολή.
- Find... (Ζωντανή Αναζήτηση): Άμεσο φιλτράρισμα γραμμών με αναζήτηση κειμένου, IP, CIDR, ή σχολίου.
- Κουμπιά ▲/▼ (Αναδιάταξη): Αλλάζουν τη σειρά εκτέλεσης (Rule Order) μετακινώντας τον κανόνα πάνω ή κάτω.

2.2 Παράμετροι Φόρμας Κανόνα (Rule Modal)

- Chain: Το αλφαριθμητικό όνομα της αλυσίδας (π.χ. bgp-in, bgp-out, Internal, isp-primary).
- Rule Order: Αριθμός προτεραιότητας εκτέλεσης (1 - 65535). Προτείνεται βήμα 10 (10, 20, 30...) για μελλοντικές παρεμβολές.
- Comment: Επεξηγηματικό σχόλιο για την τεκμηρίωση του σκοπού του κανόνα (σημειώνεται με σημαία C στον πίνακα).
- Disabled: Απενεργοποιεί τον κανόνα χωρίς να τον διαγράψει, επιτρέποντας γρήγορες δοκιμές.

2.3 Βοηθός Σύνταξης (Visual Rule Wizard) & Quick Templates

Μέσα στη φόρμα κανόνα υπάρχει πτυσσόμενος βοηθός (Visual Wizard) που επιτρέπει τη συμπλήρωση πεδίων χωρίς ανάγκη χειροκίνητης πληκτρολόγησης κώδικα:

- Prefix (CIDR): Διεύθυνση δικτύου (π.χ. 192.168.0.0/16 ή 0.0.0.0/0).
- Prefix Length: Εύρος μήκους μάσκας (π.χ. 24-32 ή ge 24).
- Protocol: Επιλογή πρωτοκόλλου προέλευσης: any, bgp, ospf, connected, static.
- Action: Επιλογή ενέργειας: accept (αποδοχή), reject (απόρριψη), passthrough (τροποποίηση & συνέχεια).
- Set Local-Pref / Prepend: Αριθμητικές τιμές για Local Preference και AS-Path Prepending.
- Generate Script Expression ↑: Μετατρέπει άμεσα τις επιλογές της φόρμας σε έγκυρο κώδικα στο κύριο πεδίο Textarea.

Έτοιμα Πρότυπα (Quick Templates):

- 0.0.0.0/0: Εισάγει ταύτιση με default route • Drop RFC1918: Απορρίπτει 10/8, 172.16/12, 192.168/16 • Len ≤ /24: Επιβάλλει όριο μήκους ≤ /24 • Loc-Pref 150: Θέτει local-pref 150 • AS-Prepend 2x: Προσθέτει 2 επαναλήψεις AS • Reject: Unconditional drop.

3. Πλήρης Οδηγός Σύνταξης Σεναρίων (Script Syntax Reference)

Το DebTik μεταφράζει αυτόματα τη σύνταξη MikroTik RouterOS v7 σε native εκφράσεις της μηχανής BIRD 2. Ακολουθεί ο αναλυτικός πίνακας όλων των υποστηριζόμενων συνθηκών και ενεργειών.

3.1 Συνθήκες Ελέγχου (Match Conditions)

Σύνταξη RouterOS v7	Σύνταξη BIRD 2	Λειτουργία & Παράδειγμα Χρήσης
`dst in A.B.C.D/M`	`net ~ [ A.B.C.D/M+ ]`	Έλεγχος αν το prefix περιέχεται στο subnet. Π.χ. dst in 10.0.0.0/8 (περιλαμβάνει /8 έως /32).
`dst in A.B.C.D/M{L,H}`	`net ~ [ A.B.C.D/M{L,H} ]`	Έλεγχος subnet με εύρος μάσκας. Π.χ. dst in 192.168.0.0/16{24,28} (υποδίκτυα /24 έως /28).
`dst == A.B.C.D/M` ή `dst = A.B.C.D/M`	`net = A.B.C.D/M`	Ακριβής ταύτιση προθέματος. Π.χ. dst == 0.0.0.0/0 (ακριβώς το default route).
`dst != A.B.C.D/M`	`net != A.B.C.D/M`	Αποκλεισμός συγκεκριμένης διαδρομής.
`dst-len == N` `dst-len <= N, >= N`	`net.len = N` `net.len <= N, >= N`	Έλεγχος μήκους προθέματος. Π.χ. net.len <= 24 αποτρέπει routes μικρότερα από /24.
`protocol <name>`	`source = RTS_<NAME>`	Έλεγχος πρωτοκόλλου: bgp (RTS_BGP), ospf (RTS_OSPF), connected (RTS_DEVICE), static (RTS_STATIC).
`bgp-communities includes A:B`	`(A, B) ~ bgp_community`	Έλεγχος αν περιέχεται συγκεκριμένο community. Π.χ. bgp-communities includes 65000:100.
`bgp-communities in ListName`	`bgp_community ~ comm_ListName`	Έλεγχος αν κάποιο community της διαδρομής ανήκει στην ορισμένη Community List.
`bgp-as-path in ListName`	`bgp_path.last ~ aslist_ListName`	Έλεγχος αν το γειτονικό AS ανήκει στη συγκεκριμένη AS List.
`bgp-as-path "pattern"`	`bgp_path ~ [= * pattern * =]`	Αντιστοίχιση διαδρομής AS με regex. Π.χ. bgp-as-path "^65000_".
`&&, ||, !`	`&&, ||, !`	Λογικοί τελεστές: AND (&&), OR (||), NOT (!).

3.2 Ενέργειες & Τροποποίηση Ιδιοτήτων (Actions & Set Attributes)

Ενέργεια (Action / Set)	Σύνταξη BIRD 2	Περιγραφή & Επίπτωση στη Δρομολόγηση
`accept;`	`accept;`	Τερματική αποδοχή. Η διαδρομή γίνεται δεκτή και σταματά η αξιολόγηση του φίλτρου.
`reject; / discard;`	`reject;`	Τερματική απόρριψη. Η διαδρομή απορρίπτεται και σταματά η αξιολόγηση του φίλτρου.
`passthrough;`	(non-terminal)	Μη-τερματική ενέργεια. Εκτελεί τις αλλαγές (set) και συνεχίζει στους επόμενους κανόνες.
`set bgp-local-pref <N>;`	`bgp_local_pref = <N>;`	BGP Local Preference (default 100). Υψηλότερη τιμή = προτιμητέα έξοδος από το AS μας.
`set bgp-med <N>;`	`bgp_med = <N>;`	BGP Multi-Exit Discriminator (MED). Χαμηλότερη τιμή = υπόδειξη εισόδου προς το γειτονικό AS.
`set bgp-path-prepend <N>;`	`bgp_path.prepend(...);`	Προσθέτει 1-10 φορές το τοπικό AS στο AS Path για αποθάρρυνση κίνησης (Backup uplink).
`set bgp-communities.add <A:B>;`	`bgp_community.add((A,B));`	Προσθέτει Community στη διαδρομή χωρίς να διαγράψει τα ήδη υπάρχοντα.
`set bgp-communities.delete <A:B>;`	`bgp_community.delete((A,B));`	Αφαιρεί συγκεκριμένο Community από τη διαδρομή.
`set distance <N>;`	`preference = <N>;`	Administrative Distance / Preference στον τοπικό πίνακα δρομολόγησης.
`set gw <IP>;`	`gw = <IP>;`	Εξαναγκαστική αλλαγή Next-Hop IP gateway της διαδρομής.

4. Ονομαστικές Λίστες (Community Lists & AS Lists)

Οι ονομαστικές λίστες επιτρέπουν την ομαδοποίηση παραμέτρων BGP (Communities και AS Numbers), διατηρώντας τα φίλτρα συνοπτικά, ευανάγνωστα και εύκολα στη συντήρηση.

4.1 BGP Community Lists (/routing filter community-list)

Τα BGP Communities είναι 32-bit ετικέτες που συνοδεύουν τις διαδρομές. Χρησιμοποιούνται για σήμανση πολιτικής, επιλογή uplink, blackholing ή γεωγραφικό διαχωρισμό.

- List Name: Το όνομα αναφοράς της λίστας (π.χ. AWMN_COMM, UPSTREAM_BLACKHOLE).
- Communities: Τιμές χωρισμένες με κόμμα σε μορφή AS:Value ή γνωστές λέξεις (no-export, blackhole). Π.χ. 65000:100, 6610:200, no-export.
- RegExp: Προαιρετικό regex μοτίβο για ταύτιση communities.
- Comment & Disabled: Περιγραφή και ενεργοποίηση/απενεργοποίηση.

Παράδειγμα Διαμόρφωσης & Μετάφρασης στο BIRD 2:

```
# 1. Ορισμός στο DebTik Web UI (Community List: AWMN_COMM):
#    Name: AWMN_COMM | Communities: 65000:100, 6610:200
#
# 2. Παραγόμενος BIRD 2 κώδικας στο /etc/bird/bird.conf:
define comm_AWMN_COMM = [ (65000, 100), (6610, 200) ];

# 3. Χρήση σε κανόνα φίλτρου (RouterOS v7 syntax):
if (bgp-communities in AWMN_COMM) {
    set bgp-local-pref 150;
    accept;
}
```

4.2 AS Number Lists (/routing filter num-list)

Οι AS Lists ορίζουν ομάδες αυτόνομων συστημάτων (AS Numbers). Επιτρέπουν τον έλεγχο προέλευσης μιας διαδρομής ή της διέλευσής της από συγκεκριμένους τηλεπικοινωνιακούς παρόχους.

- List Name: Το όνομα της λίστας (π.χ. TIER1_ISPS, GRNET_PEERS).
- Range: Εύρη με παύλα (π.χ. 65000-65010) ή μεμονωμένα ASNs χωρισμένα με κόμμα (π.χ. 6610, 17244, 3356).
- Comment & Disabled: Περιγραφή και ενεργοποίηση/απενεργοποίηση.

Παράδειγμα Διαμόρφωσης & Μετάφρασης στο BIRD 2:

```
# 1. Ορισμός στο DebTik Web UI (AS List: TIER1_ISPS):
#    Name: TIER1_ISPS | Range: 65000-65010, 6610, 17244, 3356
#
# 2. Παραγόμενος BIRD 2 κώδικας στο /etc/bird/bird.conf:
define aslist_TIER1_ISPS = [ 65000..65010, 6610, 17244, 3356 ];

# 3. Χρήση σε κανόνα φίλτρου (έλεγχος γειτονικού AS):
if (bgp-as-path in TIER1_ISPS) {
    set bgp-local-pref 200;
    accept;
}
```

ΤΕΧΝΙΚΗ ΛΕΠΤΟΜΕΡΕΙΑ: Στο BIRD 2, τα defines (comm_... και aslist_...) γράφονται στην αρχή του αρχείου /etc/bird/bird.conf πριν από τους ορισμούς των συναρτήσεων και των πρωτοκόλλων. Αυτό εξασφαλίζει ότι είναι καθολικά διαθέσιμα σε όλες τις αλυσίδες φίλτρων.

5. Σύνδεση με BGP Peering (InFilter, OutFilter & Export Policy)

Η σύνδεση μιας αλυσίδας κανόνων με ένα BGP Peer γίνεται μέσα από τη φόρμα επεξεργασίας του peer (Routing → BGP Routing → Peers), στα πεδία In-Filter και Out-Filter.

5.1 In-Filter (Εισερχόμενη Πολιτική - Import Policy)

- Σκοπός: Φιλτράρισμα των διαδρομών που λαμβάνονται από τον γείτονα πριν εισαχθούν στον πίνακα master4.
- Λειτουργία: Κάθε εισερχόμενη ενημέρωση (BGP Update) αξιολογείται από την αλυσίδα του In-Filter.
- Αποτέλεσμα: Αν εκτελεστεί accept;, η διαδρομή εγκαθίσταται. Αν εκτελεστεί reject; ή αν δεν ταιριάξει σε κανέναν κανόνα (unmatched), απορρίπτεται (Default Deny).
- Χρήση: Ιδανικό για προστασία από Route Leaks, αποκλεισμό Bogons/RFC1918 και επιβολή Local Preference ανά uplink.

5.2 Out-Filter (Εξερχόμενη Πολιτική - Export Policy) & Αυτόματη Προστασία

Στο BIRD 2, όταν οριστεί Out-Filter, όλες οι υποψήφιες διαδρομές του router περνούν από αυτό. Στο DebTik (v1.3.11+), για να αποτραπεί η ακούσια απόρριψη των δικών μας ανακοινώσεων, το Export Filter δομείται σε 3 διαδοχικά επίπεδα προτεραιότητας:

Επίπεδο Προτεραιότητας	Μηχανισμός BIRD 2	Περιγραφή & Συμπεριφορά
Επίπεδο 1: User Policy	`fn_filter_<Chain>();`	Απόλυτη προτεραιότητα. Εκτελούνται πρώτα οι κανόνες του χρήστη. Αν ένας κανόνας κάνει reject;, η διαδρομή κόβεται άμεσα. Αν κάνει accept;, εξάγεται άμεσα με τις όποιες τροποποιήσεις (prepend/community).
Επίπεδο 2: Advertised Nets	`if proto = "bgp_nets_..." then accept;`	Αυτόματη προστασία. Αν μια διαδρομή δεν ταίριαξε στους κανόνες του χρήστη, αλλά ανήκει στα Output Networks του peer ή στα BGP Networks (Blackhole static), γίνεται αυτόματα accept και ανακοινώνεται!
Επίπεδο 3: Redistribution	`if source = RTS_DEVICE then accept;` `if source ~ [ RTS_STATIC ]...`	Αναδιανομή. Αν ο χρήστης έχει τσεκάρει Redistribute Connected ή Redistribute Static, οι διαδρομές αυτές εξάγονται αυτόματα εφόσον δεν απορρίφθηκαν από το Επίπεδο 1.
Default Deny	`reject;`	Οποιαδήποτε άλλη διαδρομή δεν καλύπτεται από τα παραπάνω 3 επίπεδα απορρίπτεται με ασφάλεια.

Παράδειγμα Παραγόμενου BIRD 2 Export Configuration:

```
# Παραγόμενος κώδικας για BGP Peer με OutFilter: "Internal"
protocol bgp bgp_bgp_peer_1 {
    description "ebgp-internal-Primcast";
    local 192.168.129.226 as 65001;
    neighbor 192.168.129.225 as 65555;
    ipv4 {
        import filter filter_Internal;
        export filter {
            # Επίπεδο 1: Εκτέλεση κανόνων φίλτρου χρήστη
            fn_filter_Internal();
            # Επίπεδο 2: Αυτόματη προστασία ρητά δηλωμένων δικτύων peer & static
            if proto = "bgp_nets_bgp_bgp_peer_1" then accept;
            if proto = "bgp_static_nets" then accept;
            # Επίπεδο 3: Αναδιανομή Connected & Static (αν ενεργοποιημένη)
            if source = RTS_DEVICE then accept;
            if source ~ [ RTS_STATIC, RTS_INHERIT ] then accept;
            # Default Deny
            reject;
        };
    };
}
```

6. Πρακτικές Συνταγές & Παραδείγματα (Recipes)

Ακολουθούν 4 έτοιμα, δοκιμασμένα σενάρια διαμόρφωσης για πραγματικά περιβάλλοντα παραγωγής.

Συνταγή 1: eBGP Inbound Filter Παρόχου (Ασφαλές Edge)

Στόχος: Αποδοχή μόνο έγκυρων διαδρομών διαδικτύου, απόρριψη bogons / RFC1918 και αποδοχή default route:

```
# Chain: isp-in | Rule 10: Αποδοχή Default Route (0.0.0.0/0)
if (dst == 0.0.0.0/0) { accept; }

# Chain: isp-in | Rule 20: Απόρριψη ιδιωτικών διευθύνσεων RFC1918 & Martians
if (dst in 10.0.0.0/8 || dst in 172.16.0.0/12 || dst in 192.168.0.0/16 || dst in 127.0.0.0/8) { reject; }

# Chain: isp-in | Rule 30: Απόρριψη υπερβολικά εξειδικευμένων διαδρομών (> /24)
if (net.len > 24) { reject; }

# Chain: isp-in | Rule 40: Αποδοχή όλων των υπόλοιπων δημοσίων routes με Local-Pref 100
if (true) { set bgp-local-pref 100; accept; }
```

Συνταγή 2: Traffic Engineering (Active / Backup Upstream με AS-Prepend)

Στόχος: Προτίμηση του ISP-A για εισερχόμενη & εξερχόμενη κίνηση. Ο ISP-B χρησιμοποιείται ως εφεδρικός (Failover):

```
# Στο ISP-A Inbound (Chain: isp-a-in): Υψηλό Local-Pref 200 (Προτίμηση Εξόδου)
if (true) { set bgp-local-pref 200; accept; }

# Στο ISP-B Inbound (Chain: isp-b-in): Χαμηλό Local-Pref 100 (Εφεδρική Έξοδος)
if (true) { set bgp-local-pref 100; accept; }

# Στο ISP-B Outbound (Chain: isp-b-out): AS Prepend 2x (Αποθάρρυνση Εισόδου από ISP-B)
if (dst in 192.168.130.0/24 || dst in 192.168.131.0/24) {
    set bgp-path-prepend 2;
    accept;
}
```

Συνταγή 3: Χρήση Passthrough για Σήμανση με BGP Communities

Στόχος: Σήμανση τοπικών δικτύων με κοινοτικό αναγνωριστικό χωρίς διακοπή της αλυσίδας:

```
# Chain: customer-out | Rule 10: Passthrough σήμανση με community
if (dst in 100.64.0.0/16) {
    set bgp-communities.add 65000:500;
    passthrough;
}

# Chain: customer-out | Rule 20: Τελική αποδοχή
if (dst in 100.64.64.0/24) { accept; }
```

Συνταγή 4: Remote Triggered Blackhole (RTBH / DDoS Mitigation)

Στόχος: Άμεση απόρριψη IP υπό επίθεση μέσω ανακοίνωσης Blackhole Community στον upstream πάροχο:

```
# Chain: isp-out | Rule 5: Ανακοίνωση RTBH /32 προς upstream provider
if (dst == 192.168.131.100/32) {
    set bgp-communities.add 65535:666;  # Well-known Blackhole Community
    set gw 192.0.2.1;                   # Discard Next-Hop
    accept;
}
```

7. Διαγνωστικά, CLI Troubleshooting & FAQ

Το DebTik παρέχει πλήρη εποπτεία της λειτουργίας των φίλτρων τόσο μέσω του γραφικού περιβάλλοντος όσο και μέσω της διεπαφής γραμμής εντολών του BIRD 2 (birdc).

7.1 Εντολές Ελέγχου BIRD CLI (birdc)

Εντολή CLI	Περιγραφή & Χρησιμότητα Ελέγχου
`birdc show protocols`	Συνοπτική κατάσταση όλων των πρωτοκόλλων (BGP, OSPF, Static), uptime και κατάσταση (Established/Active/Idle).
`birdc show protocols all <peer>`	Κύρια διαγνωστική εντολή. Εμφανίζει στατιστικά φίλτρων: Import updates, rejected, filtered, accepted και Export updates, rejected, accepted.
`birdc show route export <peer>`	Εμφανίζει ακριβώς ποιες διαδρομές ανακοινώνονται αυτή τη στιγμή προς το συγκεκριμένο peer μετά την εφαρμογή του Out-Filter.
`birdc show route import <peer>`	Εμφανίζει τις διαδρομές που εισήχθησαν από το peer μετά την εφαρμογή του In-Filter.
`birdc show route filtered <peer>`	Εμφανίζει ποιες διαδρομές απορρίφθηκαν από το φίλτρο.
`birdc show route for <prefix> all`	Εμφανίζει όλες τις λεπτομέρειες για ένα συγκεκριμένο subnet (AS-Path, Communities, Local Preference, Next-Hop).
`birdc restart <peer>`	Επανεκκινεί άμεσα το session με το peer για στιγμιαία επαναξιολόγηση και ανανέωση όλων των διαδρομών.

7.2 Συχνές Ερωτήσεις & Επίλυση Προβλημάτων (FAQ)

ΟΔΗΓΟΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ: Ερώτηση 1: Το peer είναι Established αλλά δεν ανακοινώνει τα static/blackhole subnets μου. Γιατί;
Απάντηση: Ελέγξτε αν έχετε ορίσει Out-Filter στο peer. Στην έκδοση 1.3.11+, τα ρητά δηλωμένα Advertised Networks (Output Networks / Static Blackhole) ανακοινώνονται αυτόματα. Επαληθεύστε εκτελώντας birdc show route export <peer> για να δείτε ακριβώς ποια prefixes αποστέλλονται στον γείτονα.

Ερώτηση 2: Έγραψα κανόνα με '==' και εμφάνιζε syntax error στο BIRD 2.
Απάντηση: Το BIRD 2 δέχεται αποκλειστικά μονό = για έλεγχο ισότητας. Το DebTik (v1.3.11+) μετατρέπει αυτόματα οποιοδήποτε == σε = κατά την αποθήκευση, προστατεύοντας από συντακτικά σφάλματα.

Ερώτηση 3: Πώς ελέγχω αν το φίλτρο απορρίπτει διαδρομές που χρειάζομαι;
Απάντηση: Εκτελέστε birdc show protocols all <peer> και κοιτάξτε τη γραμμή Route change stats → filtered. Αν ο αριθμός αυξάνεται, εκτελέστε birdc show route filtered <peer> για να δείτε τα συγκεκριμένα prefixes και να προσθέσετε κανόνα accept στο chain σας.

Ερώτηση 4: Τι συνέβη με την καρτέλα 'Select Rules';
Απάντηση: Τα Select Rules ήταν έννοια του RouterOS v7 που δεν υποστηρίζεται από το BIRD 2. Στην έκδοση 1.3.11 αφαιρέθηκαν πλήρως για την απλοποίηση και αξιοπιστία της πλατφόρμας, καθώς όλα τα routing policies υλοποιούνται πληρέστερα μέσω των Filter Rules.