perimeter-ident-01

ietf://85/homenet

ek@google.com

Scope and Terminology

- Tries to limit the scope

- Terminology
    - "interior"
      approx. a single logical administrative domain
    - "exterior"
      everything else
    - "border"
      whenever a demarcation is crossed

- Only going to deal with one of each

-00

- Product-defined interface purposes
- Routing adjacency
  - Security requirements/implications?
- Links requiring subscriber information
  - 3GPP ("valid SIM cards"), PPPoE with credentials
- Links requiring existing IP-layer connectivity
  - PPTP, L2TP, 6rd, 4rd, 6to4, Teredo
- Links that are point-to-point in nature
  - PPPo{A,E}, possible future link types

-01

- Fixed-category interfaces
- Routing adjacency
  - border security == security of the homenet routing protocol adjacency formation
  - security may be "strictly less than" if mixed mode interfaces are supported

Learning algorithm

1. Collect next hop information (continuously)
2. Classify next hops

```
for each next hop:
  internal = has_adjacency
             ? true : false
  internal = i_am_delegating_router
             ? true : internal;
  external = !internal
```

3. Classify interfaces by their next hops

⟶ Apply policies based on classifications

Filter policies: a use case

- Dynamically maintain an access list representing all current, learned, internal covering prefixes.
  - examples use `{interior_nets}`

- Use the categorization of interfaces to decide what where to apply a given policy using the internal prefixes access list

Filter policy: interior anti-spoofing

- On all interior interfaces:

1.
```
from !{interior_nets}
to   !{interior_nets} deny
```

2.
```
# probably permit all
```

Filter policy: stateful exterior

- On all exterior interfaces:

1.
   ```
   from  {interior_nets}
   to   !{interior_nets}
   permit
   ```

2.
   ```
   from !{interior_nets}
   to    {interior_nets}
   permit established
   ```

3.
   ```
   from any to any deny
   ```

Some open questions

1. Broadly: does this suffice?
2. Is the delegating router exception ok?
3. What to do about "mixed" mode interfaces?
4. RAs on external interfaces (Ole Troan)?