Dynamic IPv6 Prefix Problems and VPNs

Johannes Weber
Webernetz.net – Network Security Consulting
#whoami: Johannes Weber

- Network Security Consultant @ TÜV Rheinland i-sec GmbH
  - Firewall
  - VPN/Crypto
  - Routing/Switching
  - Mail
- IPv6
- DNSSEC
- [https://blog.webernetz.net](https://blog.webernetz.net)
- [@webernetz](https://twitter.com/webernetz)
Agenda

• Migration from IPv4 to IPv6 -> Changed Concepts/Principles
• IPv6 Site-to-Site VPNs
• IPv6 Dynamic Prefix Problems
• Examples: Screenshots from Juniper ScreenOS
  • Yes, it’s End-of-Everything
  • But: Cheap for labs, almost complete IPv6 functionalities: PPPoE w/ IPV6CP, DHCPv6-PD
  • Palo Alto Networks, Fortinet FortiGate, Cisco ASA
  • (In the meantime, FortiGate v5.4 implemented DHCPv6-PD)
• Stats: IPv6 Adoption
Wording

• Route-Based VPN Tunnels
  • Each VPN tunnel has a tunnel-interface
  • Appropriate routes into tunnel-interfaces
  • Tunnel-interfaces are bound to security-zones

• Scenarios
  • Three zones per firewall: untrust, trust, vpn(-tunnel)
  • Headquarter \(\leftrightarrow\) Remote Office / Home Office / Subsidiary / Partner
IPv6 Site-to-Site VPNs
What’s a VPN Tunnel for?

• Wikipedia: “A virtual private network (VPN) extends a private network across a public network [...]”

• “They are used to securely connect geographically separated offices of an organization [...]”

• → Traffic intended for a secure VPN tunnel MUST NOT traverse the unsecure Internet!

• Example: securing mail transfers between two partner MTAs
IPv4 Site-to-Site VPN

- Only private (RFC1918) IPv4 addresses on both sites
- Route into Tunnel Interface
- Security Policy from trust -> vpn (and vice versa)
- If VPN tunnel is down, nothing happens. At least the ISP router discards private IPv4 addresses.
- Both ends are neither addressable nor accessible
IPv6 Site-to-Site VPN

- Routable Global Unicast Addresses (GUA) on both sites
- If VPN tunnel is down, packets might traverse successfully through the (unencrypted) Internet!
- Both ends ARE addressable and possibly accessible (DMZ)
IPv6 Site-to-Site VPN Principles

1. Static and Permanent Route to other site through VPN
2. uRPF on untrust
3. Policy trust -> untrust DENY traffic to remote site
4. Policy untrust -> trust DENY traffic from remote site
Example

• End-to-End communication without VPN:

C:\Users\Johannes Weber>tracert -d lx.webernetz.net
über maximal 30 Hops:

1 1 ms 1 ms 1 ms 2003:50:aa0a:3584::1
2 3 ms 2 ms 2 ms 2003:0:1301:4205::1
3 4 ms 6 ms 6 ms 2003:0:1301:4238::2
4 6 ms 7 ms 7 ms 2003:0:1302:403::1
5 4 ms 3 ms 4 ms 2003:0:1302:403::2
6 5 ms 4 ms 4 ms 2003:51:6012::2
7 5 ms 5 ms 5 ms 2003:51:6012:110::9

Ablaufverfolgung beendet.

• And with VPN:

C:\Users\Johannes Weber>tracert -d lx.webernetz.net
über maximal 30 Hops:

1 1 ms 1 ms 1 ms 2003:50:aa0a:3584::1
2 * * * Zeitüberschreitung der Anforderung.
3 6 ms 6 ms 7 ms 2003:51:6012:110::9

Ablaufverfolgung beendet.
Broken VPN -> Still Permanent Route (RO)
Deleted Route -> Still Deny Policy (RO)
Deleted Remote Policy -> Still HQ Policy/uPRF

- Route and deny policy are deleted on remote site
- HQ still blocks connections

C:\Users\Johannes Weber>tracert -d lx.webernetz.net
über maximal 30 Hops:

1 1 ms 1 ms 1 ms 2003:50:aa0a:3584::1
2 3 ms 3 ms 3 ms 2003:0:1301:4205::1
3 7 ms 4 ms 5 ms 2003:0:1301:4238::2
4 6 ms 18 ms 16 ms 2003:0:1302:403::1
5 3 ms 3 ms 3 ms 2003:0:1302:403::2
6 * * * Zeitüberschreitung der Anforderung.
7 * * * Zeitüberschreitung der Anforderung.
8 * * * Zeitüberschreitung der Anforderung.
Deleted Remote Policy -> Still HQ uRPF
Deleted Remote Policy -> Still HQ Policy

<table>
<thead>
<tr>
<th>ID</th>
<th>Source Address/Port</th>
<th>Destination Address/Port</th>
<th>Translated Source Address/Port</th>
<th>Translated Destination Address/Port</th>
<th>Service</th>
<th>Duration</th>
<th>Bytes Sent</th>
<th>Bytes Received</th>
<th>Close Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>277</td>
<td>Untrust/2003:50:a00a:3584::64</td>
<td>DMZ/Any-IPv6 ANY</td>
<td>0.0.0.0:0</td>
<td>0.0.0.0:0</td>
<td>ICMPv6</td>
<td>0 sec.</td>
<td>72</td>
<td>Traffic Denied</td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>Untrust/2003:50:a00a:3584::64</td>
<td>DMZ/Any-IPv6 ANY</td>
<td>0.0.0.0:0</td>
<td>0.0.0.0:0</td>
<td>ICMPv6</td>
<td>0 sec.</td>
<td>40</td>
<td>Traffic Denied</td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>Untrust/2003:50:a00a:3584::64</td>
<td>DMZ/Any-IPv6 ANY</td>
<td>0.0.0.0:0</td>
<td>0.0.0.0:0</td>
<td>ICMPv6</td>
<td>0 sec.</td>
<td>72</td>
<td>Traffic Denied</td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>Untrust/2003:50:a00a:3584::64</td>
<td>DMZ/Any-IPv6 ANY</td>
<td>0.0.0.0:0</td>
<td>0.0.0.0:0</td>
<td>ICMPv6</td>
<td>0 sec.</td>
<td>40</td>
<td>Traffic Denied</td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>Untrust/2003:50:a00a:3584::64</td>
<td>DMZ/Any-IPv6 ANY</td>
<td>0.0.0.0:0</td>
<td>0.0.0.0:0</td>
<td>ICMPv6</td>
<td>0 sec.</td>
<td>72</td>
<td>Traffic Denied</td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>Untrust/2003:50:a00a:3584::64</td>
<td>DMZ/Any-IPv6 ANY</td>
<td>0.0.0.0:0</td>
<td>0.0.0.0:0</td>
<td>ICMPv6</td>
<td>0 sec.</td>
<td>40</td>
<td>Traffic Denied</td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>Untrust/2003:50:a00a:3584::64</td>
<td>DMZ/Any-IPv6 ANY</td>
<td>0.0.0.0:0</td>
<td>0.0.0.0:0</td>
<td>ICMPv6</td>
<td>0 sec.</td>
<td>72</td>
<td>Traffic Denied</td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>Untrust/2003:50:a00a:3584::64</td>
<td>DMZ/Any-IPv6 ANY</td>
<td>0.0.0.0:0</td>
<td>0.0.0.0:0</td>
<td>ICMPv6</td>
<td>0 sec.</td>
<td>40</td>
<td>Traffic Denied</td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>Untrust/2003:50:a00a:3584::64</td>
<td>DMZ/Any-IPv6 ANY</td>
<td>0.0.0.0:0</td>
<td>0.0.0.0:0</td>
<td>ICMPv6</td>
<td>0 sec.</td>
<td>72</td>
<td>Traffic Denied</td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>Untrust/2003:50:a00a:3584::64</td>
<td>DMZ/Any-IPv6 ANY</td>
<td>0.0.0.0:0</td>
<td>0.0.0.0:0</td>
<td>ICMPv6</td>
<td>0 sec.</td>
<td>40</td>
<td>Traffic Denied</td>
<td></td>
</tr>
</tbody>
</table>
IPv6 Site-to-Site VPN - Conclusion

- With these four principles/recommendations it is possible to ensure that IPv6 traffic which should only traverse through a secure VPN connection won’t ever traverse through the Internet, even in case of a VPN failure on any of those sites.
- They furthermore ensure, that security is not made only at the network layer (routing), but at a firewall stage (policy).
- Questions so far?
Dynamic IPv6 Prefix Problems
Dynamic Prefix/Address Assumptions

• Quite common on private ISP connections in Germany
• „Zwangstrennung“ every 6 month (formerly every 24 hours)
• And after every reboot of the router
• → Customers are using those cheap ISP connections for home offices, trade fairs, mobile stands, distributed disaster recovery offices, ...
• And of course: IT admins at home ;)
• For the remainder of this talk:
  • GUAs, not ULAs (no NAT/NPT/othershit!)
  • Local breakouts (due to bandwidth; NextGen-Firewalls, APT-Sensors)
(1) Multiple DNS Updates

IPv4

Internet

IPv6

Internet

Single IPv4 address DNS update

Multiple IPv6 addresses DNS updates

IPv6 Prefix
(1) Multiple DNS Updates -> Solution?
(2) FQDN-based Security Policies

IPv4
- SOHO
  - Dyn DNS: fqdn.foo.bar
- Internet
- Headquarter
  - Allow fqdn.foo.bar

IPv6
- SOHO
  - Dyn Prefix: ???
- Internet
- Headquarter
  - Allow dyn prefix ??NOT SOLVED!!
(2) FQDN-based Security Policies -> Solution?

- DNS Resource Records „APL“, Lists of Address Prefixes, RFC 3123
- `ipv6-doc.weberdns.de. IN APL 2:2001:db8::/32`
- Only „experimental“ <- in fact: not used anywhere

- Small challenge everyone?
- What‘s the APL of `tr18.weberdns.de`?
(2) FQDN-based Security Policies -> Solution?

• Another idea: Shifting the prefix length on FQDN objects
• E.g.: One device updates its /128 IPv6 DNS name
• Firewall interprets this object as a /56
• Not used anywhere, too
(3) Routing into VPN Tunnels & Solution!

IPv4

SOHO

Internet

Headquarter

RFC 1918
Private IPv4 Addresses

VPN Tunnel

Static Route

IPv6

SOHO

Internet

Headquarters

RFC 1918
Private IPv4 Addresses

VPN Tunnel

Static Route

Dynamic Prefix

Dynamic Routing Protocol or
Static Route

Dynamic Routing Protocol

Static IPv6 Addresses
(3) Routing into VPN Tunnels Example HQ

<table>
<thead>
<tr>
<th>IP/Prefix</th>
<th>Gateway</th>
<th>Interface</th>
<th>Protocol</th>
<th>Preference</th>
<th>Metric</th>
<th>Vsys</th>
<th>Description</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 2003:51:6012:140::/64</td>
<td>2003:51:6012:101::4</td>
<td>ethernet0/6</td>
<td>S</td>
<td>20</td>
<td>1</td>
<td>Root</td>
<td></td>
<td>Remove</td>
</tr>
<tr>
<td>* ::/0</td>
<td>2003:51:6012::1</td>
<td>ethernet0/1</td>
<td>SP</td>
<td>20</td>
<td>1</td>
<td>Root</td>
<td></td>
<td>Remove</td>
</tr>
<tr>
<td>* 2003:51:6012:2/64</td>
<td>::</td>
<td>ethernet0/1</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2003:51:6012:2/128</td>
<td>::</td>
<td>ethernet0/1</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2003:51:6012:110::1/64</td>
<td>::</td>
<td>ethernet0/1</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2003:51:6012:110::1/128</td>
<td>::</td>
<td>ethernet0/1</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2003:51:6012:101::1/64</td>
<td>::</td>
<td>ethernet0/1</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2003:51:6012:101::1/128</td>
<td>::</td>
<td>ethernet0/1</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003:51:6012:101::64</td>
<td>::</td>
<td>ethernet0/6</td>
<td>O</td>
<td>60</td>
<td>100</td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003:51:6012:101::64</td>
<td>::</td>
<td>ethernet0/6</td>
<td>O</td>
<td>60</td>
<td>100</td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2003:50:aa0c:1300::/64</td>
<td>fe80::fce5:40ff:fe14:1</td>
<td>tunnel.2</td>
<td>O</td>
<td>60</td>
<td>10100</td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2003:50:aa0c:1342:b2c6:9aff:fedf:ca97/128</td>
<td>fe80::fce5:40ff:fe14:1</td>
<td>tunnel.2</td>
<td>O</td>
<td>60</td>
<td>10000</td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2003:51:6012:102::/64</td>
<td>fe80::21a:6cffe:faa1:2b98</td>
<td>ethernet0/6</td>
<td>O</td>
<td>60</td>
<td>200</td>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2003:51:6012:130::/64</td>
<td>fe80::2a94:ffff:fe8::772d</td>
<td>ethernet0/6</td>
<td>O</td>
<td>60</td>
<td>200</td>
<td>Root</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## (3) Routing into VPN Tunnels Example RO

<table>
<thead>
<tr>
<th>IP/Prefix</th>
<th>Gateway</th>
<th>Interface</th>
<th>Protocol</th>
<th>Preference</th>
<th>Metric</th>
<th>Vsys</th>
<th>Description</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>* ::/0</td>
<td>fe80::462b:3ff:fe19:300</td>
<td>ethernet0/0</td>
<td>D</td>
<td>252</td>
<td>1</td>
<td>Root</td>
<td></td>
<td>Remove</td>
</tr>
<tr>
<td>2003:50:aa7f:8c13:b2c6:9aff:fefd:ca80/64</td>
<td>::</td>
<td>ethernet0/0</td>
<td>C</td>
<td>Root</td>
<td>-</td>
<td>-</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>2003:50:aa7f:8c13:b2c6:9aff:fefd:ca80/128</td>
<td>::</td>
<td>ethernet0/0</td>
<td>H</td>
<td>Root</td>
<td>-</td>
<td>-</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>2003:50:aa0c:1300:b2c6:9aff:fefd:ca8c/64</td>
<td>::</td>
<td>bgroup1</td>
<td>H</td>
<td>Root</td>
<td>-</td>
<td>-</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>2003:50:aa0c:1300:b2c6:9aff:fefd:ca8c/128</td>
<td>::</td>
<td>bgroup1</td>
<td>H</td>
<td>Root</td>
<td>-</td>
<td>-</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>2003:51:6012:101::/64</td>
<td>fe80::d2f:0ff:fe14:2</td>
<td>tunnel.1</td>
<td>O</td>
<td>60</td>
<td>10100</td>
<td>Root</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>2003:51:6012:110::/64</td>
<td>fe80::d2f:0ff:fe14:2</td>
<td>tunnel.1</td>
<td>O</td>
<td>60</td>
<td>10100</td>
<td>Root</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>2003:50:aa0c:1342:b2c6:9aff:fefd:ca97/64</td>
<td>::</td>
<td>wireless0/2</td>
<td>C</td>
<td>Root</td>
<td>-</td>
<td>-</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>2003:50:aa0c:1342:b2c6:9aff:fefd:ca97/128</td>
<td>::</td>
<td>wireless0/2</td>
<td>H</td>
<td>Root</td>
<td>-</td>
<td>-</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>2003:51:6012:102::/64</td>
<td>fe80::d2f:0ff:fe14:2</td>
<td>tunnel.1</td>
<td>O</td>
<td>60</td>
<td>10200</td>
<td>Root</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>2003:51:6012:130::/64</td>
<td>fe80::d2f:0ff:fe14:2</td>
<td>tunnel.1</td>
<td>O</td>
<td>60</td>
<td>10200</td>
<td>Root</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>2003:51:6012:160::/64</td>
<td>fe80::d2f:0ff:fe14:2</td>
<td>tunnel.1</td>
<td>O</td>
<td>60</td>
<td>10200</td>
<td>Root</td>
<td></td>
<td>-</td>
</tr>
</tbody>
</table>
(3) Routing into VPN Tunnels & Solution?

• Another possible solution: Two prefixes on the link
  • A) dynamic prefix from the ISP
  • B) static prefix from the HQ through VPN tunnel
  • But „Source-Address-Dependent Routing“ brings other problems! (RFC 8043)

• Or: ULAs with NPT
Dynamic IPv6 Prefix Problems - Conclusion

• Yes, IPv6 solves the address problem
• Yes, you can greatly structure your address plan
• BUT: Common workarounds for „dynamic IPv4 addresses“ do NOT work for „dynamic IPv6 prefixes“!
Dynamic IPv6 Prefix Problems - Conclusion

- Go for static/persistent IPv6 prefixes!
- At least in customer environments
- If not: you have to deal with it ;(
- RIPE 690 Best Current Operational Practice for Operators:
  - "Non-persistent prefixes are considered harmful in IPv6 as you can't avoid issues that may be caused by simple end-user power outages, so assigning persistent prefixes is a safer and simpler approach."
  - "Trying to deploy new services or applications with non-persistent prefixes is always more difficult and costly, and will increase time spent on troubleshooting."
- Go for static/persistent IPv6 prefixes!
Questions? Comments?

johannes@webernetz.net
https://blog.webernetz.net/ipv6
@webernetz