Simple Security in IPv6 Residential Gateway CPE

draft-ietf-v6ops-cpe-simple-security

james woodyatt <jhw@apple.com>

Motivation

Motivation

- RFC 4864, Local Network Protection for IPv6, recommends simple security for residential gateways.

Motivation

- RFC 4864, Local Network Protection for IPv6, recommends simple security for residential gateways.
- Does not go into much detail.

Motivation

- RFC 4864, Local Network Protection for IPv6, recommends simple security for residential gateways.
- Does not go into much detail.
- Just says, basically, outbound flows to be generally allowed and inbound flows to be generally refused.

Motivation

- RFC 4864, Local Network Protection for IPv6, recommends simple security for residential gateways.
- Does not go into much detail.
- Just says, basically, outbound flows to be generally allowed and inbound flows to be generally refused.
- Applications developers to benefit if vendors of residential CPE have more detailed recommendations.

Scenario Overview

Scenario Overview

- Routing for home and very small office use.

Scenario Overview

- Routing for home and very small office use.
- May be deployed by users with no significant expertise in internetworking.

Scenario Overview

- Routing for home and very small office use.
- May be deployed by users with no significant expertise in internetworking.
- May be integrated with IPv4/NAT functions that users are familiar with today.

Scenario Overview

- Routing for home and very small office use.
- May be deployed by users with no significant expertise in internetworking.
- May be integrated with IPv4/NAT functions that users are familiar with today.
- IPv6 simple security intended to be functionally similar to IPv4/NAT simple security.

Similarities with IPv4/NAT

Similarities with IPv4/NAT

- Filtering behaviors for TCP and UDP as recommended by BEHAVE for IPv4/NAT. ICMP is RFC 4890.

Similarities with IPv4/NAT

- Filtering behaviors for TCP and UDP as recommended by BEHAVE for IPv4/NAT. ICMP is RFC 4890.
- Some application protocols, e.g. FTP, RTSP, SIP, want transparency helpers. Not discussed in the draft.

Similarities with IPv4/NAT

- Filtering behaviors for TCP and UDP as recommended by BEHAVE for IPv4/NAT. ICMP is RFC 4890.
- Some application protocols, e.g. FTP, RTSP, SIP, want transparency helpers. Not discussed in the draft.
- Alternatively, techniques like STUN and TURN will work.

Similarities with IPv4/NAT

- Filtering behaviors for TCP and UDP as recommended by BEHAVE for IPv4/NAT. ICMP is RFC 4890.
- Some application protocols, e.g. FTP, RTSP, SIP, want transparency helpers. Not discussed in the draft.
- Alternatively, techniques like STUN and TURN will work.
- Hole-punching for passive listeners, i.e. UPnP IGD or its alternatives. Not much in this draft about them.

Special IPv6 Considerations

james woodyatt <jhw@apple.com>

Special IPv6 Considerations

- Teredo blocked to prevent bypassing simple security.

Special IPv6 Considerations

- Teredo blocked to prevent bypassing simple security.
- IPsec AH, ESP and IKE allowed.

Special IPv6 Considerations

- Teredo blocked to prevent bypassing simple security.
- IPsec AH, ESP and IKE allowed.
- UDP-lite, SCTP and DCCP stateful filtering.

Special IPv6 Considerations

- Teredo blocked to prevent bypassing simple security.
- IPsec AH, ESP and IKE allowed.
- UDP-lite, SCTP and DCCP stateful filtering.
- 3-tuple states for unrecognized upper-layer transport.

Recent Updates

Recent Updates

- Removed default-allow for GRE and IP-in-IP.

Recent Updates

- Removed default-allow for GRE and IP-in-IP.
- Tweaked the recommendation about passive listeners.

Recent Updates

- Removed default-allow for GRE and IP-in-IP.
- Tweaked the recommendation about passive listeners.
- No management on WAN for *subscriber-managed* gateways.

Recent Updates

- Removed default-allow for GRE and IP-in-IP.
- Tweaked the recommendation about passive listeners.
- No management on WAN for *subscriber-managed* gateways.
- Added a some normative and informative references.

Recent Updates

- Removed default-allow for GRE and IP-in-IP.
- Tweaked the recommendation about passive listeners.
- No management on WAN for *subscriber-managed* gateways.
- Added a some normative and informative references.
- Many editorial changes.

Open Issues

Open Issues

- The authors of I-D.vyncke-advanced-ipv6-security have expressed some general concerns about the “default deny” policy inherent in CPE Simple Security.

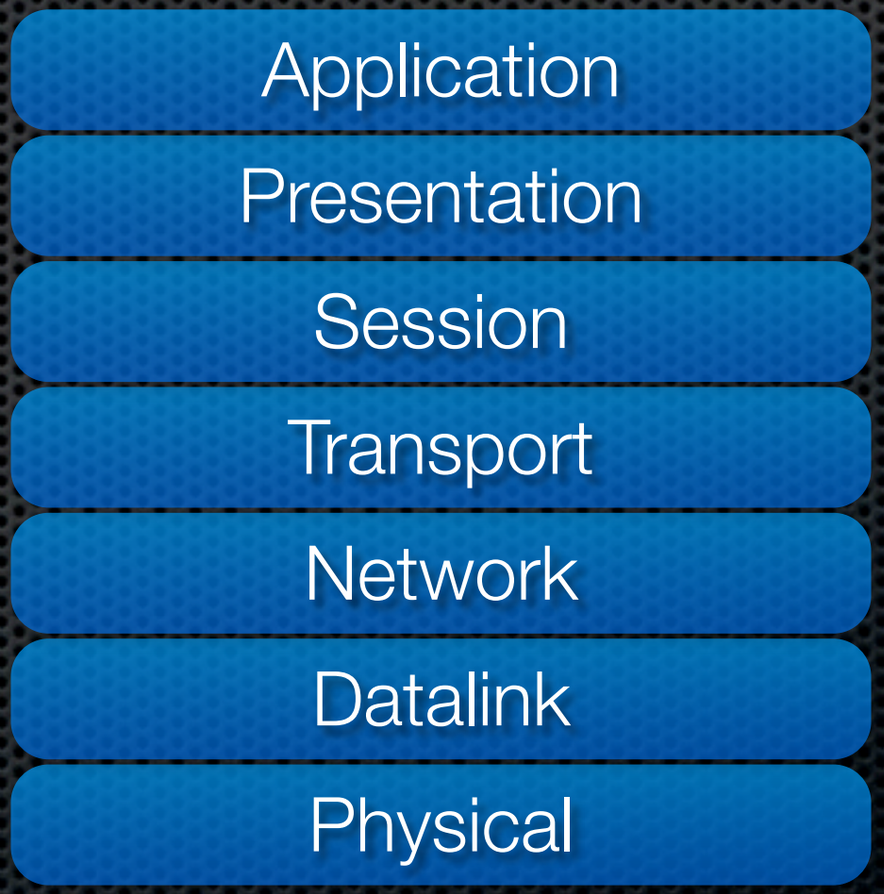
Open Issues

- The authors of I-D.vyncke-advanced-ipv6-security have expressed some general concerns about the “default deny” policy inherent in CPE Simple Security.
- Are there any other remaining troubles?

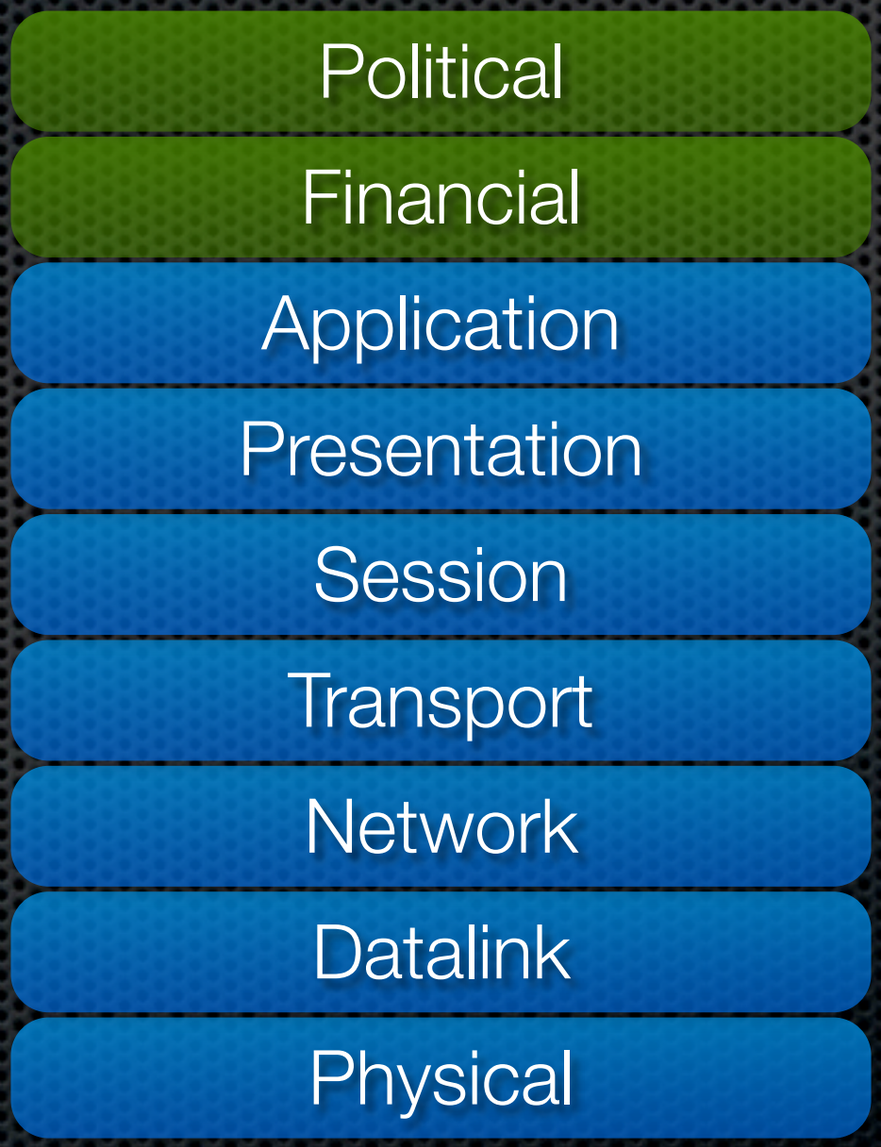
The IETF Protocol Stack

james woodyatt <jhw@apple.com>

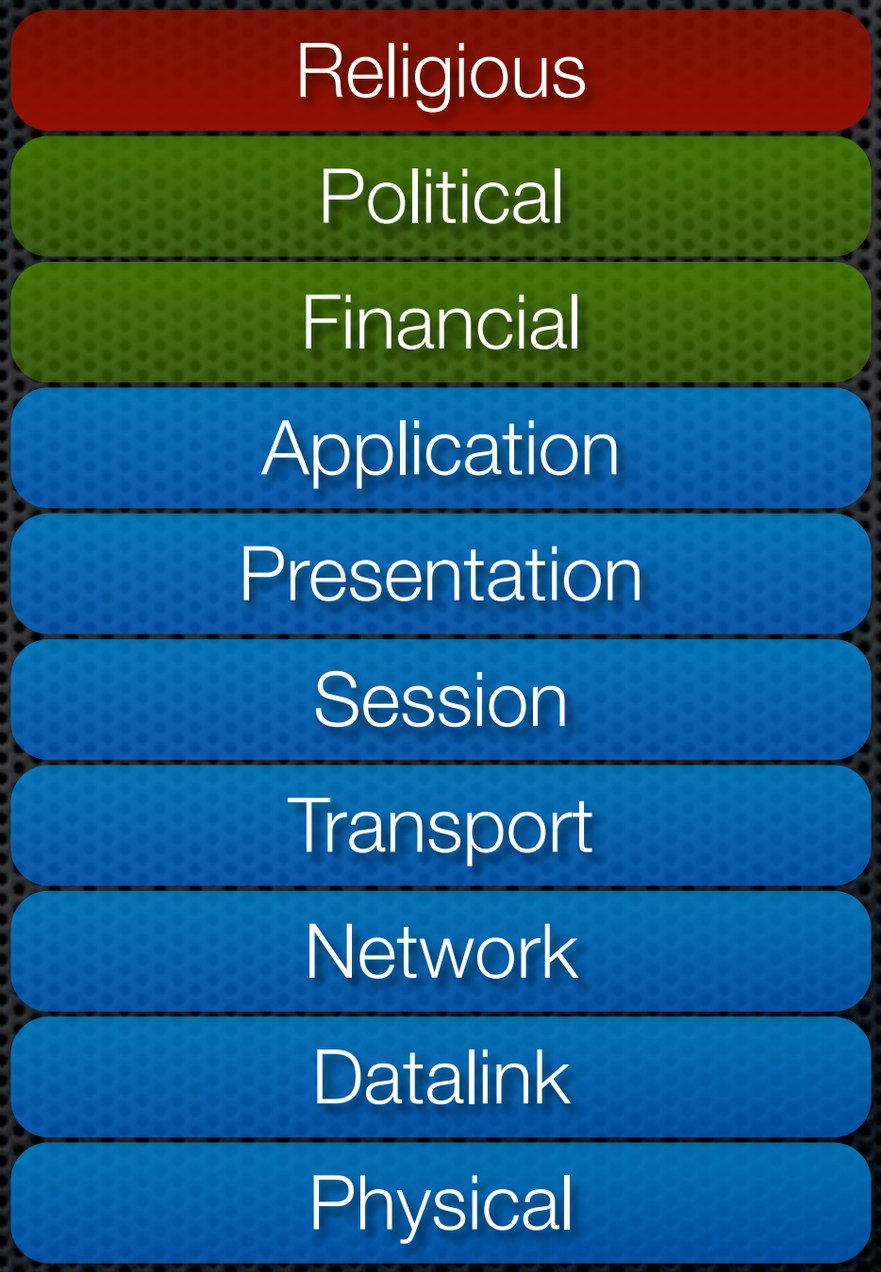
The IETF Protocol Stack



The IETF Protocol Stack



The IETF Protocol Stack



The IETF Protocol Stack