DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers

(draft-gont-opsec-dhcpv6-shield)

Fernando Gont

SI6 NETWORKS

IETF 84
Vancouver, Canada. July 29-August 3, 2012

Overview

- DHCPv6-Shield is the IPv6 version of “DHCP-snooping”
- Aims at blocking malicious DHCPv6-server packets at layer-2
    - Only DHCPv6-server packets received on a specific port will be allowed
- **Complements other technologies such as RA-Guard**

draft-gont-opsec-dhcpv6-shield

- Specifies the filtering rules for DHCPv6-Shield
- Greatly benefits from work done in v6ops for RA-Guard
    - draft-ietf-v6ops-ra-guard-implementation

Filtering rules

Filtering rules to be applied on non-DHCPv6-server ports:

1. Follow the entire IPv6 header chain to identify DHCPv6-server packets
2. If the packet is a first-fragment and the upper-layer header is not found, drop the packet
3. If the packet is a DHCPv6-server packet, drop the packet
4. Otherwise, pass the packet as usual

Moving forward

- Adopt as an OPSEC WG item?

Thanks!

Fernando Gont

fgont@si6networks.com

www.si6networks.com