Schema

title:	Stateless Packet Filtering
module:	oasis-open.org/openc2/v1.0/ap-slpf
version:	wd03
description:	Data definitions for Stateless Packet Filtering (SLPF) functions
exports:	Target, Specifiers, Args, Results

3.2 Structure Types

3.2.1 Target

SLPF targets

Target (Choice)

ID	Name	Type	Description
1	rule	Rule-ID	Uniquely identifies a rule associated with a previously-issued deny or allow.

3.2.2 Specifiers

SLPF actuator specifiers

Specifiers (Map)

ID	Name	Type	#	Description
1	nfv_id	String	1	Identifier of a virtualized packet filter

3.2.3 Args

SLPF command arguments

Args (Map)

ID	Name	Type	#	Description
1	drop_process	Drop-Process	0..1	How to handle denied packets
2	running	Boolean	0..1	Normal operation assumes updates are persistent. If TRUE, updates are not persistent in the event of a reboot or restart. Default=FALSE.
3	direction	Direction	0..1	Specifies direction (ingress or egress) for allow or deny rules. If omitted rules affact all traffic.
4	insert_rule	Integer	1	Specifies the identifier of the rule within a list, typically used in a top-down rule list.

3.2.4 Drop-Process

Drop-Process (Enumerated)

ID	Name	Description
1	None	Drop the packet and do not send a notification to the source of the packet.
2	Reject	Drop the packet and send an ICMP host unreachable (or equivalent) to the source of the packet.
3	False_ack	Drop the packet and send a false acknowledgement that the packet was received [???].

3.2.5 Direction

Direction (Enumerated)

ID	Name	Description
1	ingress	Apply rules to incoming traffic only
2	egress	Apply rule to outbound traffic only

3.2.6 Results

SLPF results

Results (Map)

ID	Name	Type	#	Description
1	rule	Rule-ID	0..1	Rule identifier returned from allow or deny command.

3.3 Primitive Types

Name	Type	Description
Rule-ID	Integer	Immutable identifier assigned when an access rule is created.