Schema

title: Stateless Packet Filtering
module: oasis-open.org/openc2/oc2slpf/v1.0/oc2slpf-v1.0
patch: 0
description: Data definitions for Stateless Packet Filtering (SLPF) functions
exports: Target, Specifiers, Args, Results

Target (Choice)

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

Args (Map)

ID	Name	Type	#	Description
1	drop_process	Drop-Process	0..1	Specifies 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 whether to apply rules to incoming or outgoing traffic. If omitted, rules are applied to both.
4	insert_rule	Rule-ID	0..1	Specifies the identifier of the rule within a list, typically used in a top-down rule list.

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 traffic and send a false acknowledgement that the data was received by the destination.

Direction (Enumerated)

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

Rule-ID

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

Specifiers (Map)

ID	Name	Type	#	Description
1	hostname	String	0..1	RFC 1123 hostname (can be a domain name or IP address) for a particular device with SLPF functionality
2	named_group	String	0..1	User-defined collection of devices with SLPF functionality
3	asset_id	String	0..1	Unique identifier for a particular SLPF
4	asset_tuple	String	0..10	Unique tuple identifier for a particular SLPF consisting of a list of up to 10 strings

Results (Map)

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