



Firewall Inspection Requirements

- [Workflows](#)
- [Resource Summary for Firewall Inspection](#)
- [ZBFW Zone Resource](#)
- [ZBFW Filter Resource](#)
- [ZBFW Policy Resource](#)
- [Firewall Session Collection Resource](#)
- [Set Firewall High-Speed Logger Resource](#)
- [Firewall Statistics \(Global Count\) Resource](#)

Workflows

Workflow: Setting Up Firewall Inspection

Configure the firewall inspection in the following order:

1. Create a source zone.
POST /api/v1/zbfw-svc/zones
See [Create a ZBFW Zone, page 16-3](#).
2. Create a destination zone.
POST /api/v1/zbfw-svc/zones
See [Create a ZBFW Zone, page 16-3](#).
3. If an ACL is required, configure an ACL.
POST /api/v1/acl
See [Configure an ACL, page 14-9](#) and [ACL Requirements for Subnets or IP Ranges, page 14-1](#).
4. Create the firewall filter rules.
POST /api/v1/zbfw-svc/filters
See [Create a ZBFW Filter, page 16-6](#).

5. Create the firewall policy.
 POST /api/v1/zbfw-svc/policies
 See [Create a Firewall Policy](#), page 16-12.



Note

 The REST API internally generates the zone-based firewall policy-map.

Resource Summary for Firewall Inspection

Resource Summary

Resource	URL (BaseURL)	HTTP Method			
		GET	POST	PUT	DELETE
Zones A source zone and a destination zone must be created before configuring a zone-base firewall policy.	/api/v1/zbfw-svc/zones	Y	Y	N	N
	/api/v1/zbfw-svc/zones/{zone-name}	Y	N	Y	Y
Filters	/api/v1/zbfw-svc/filters	Y	Y	N	N
	/api/v1/zbfw-svc/filters/{filter-id}	Y	N	Y	Y
Policies	/api/v1/zbfw-svc/policies	Y	Y	N	N
	/api/v1/zbfw-svc/policies/<policy-id>	Y	N	Y	Y
FW global log of number of packet dropped	/api/v1/zbfw-svc/log	Y	N	Y	N
Sessions Report, including allowed traffic	/api/v1/zbfw-svc/active-sessions	Y	N	N	N
Dropped traffic and allowed traffic	/api/v1/zbfw-svc/statistics	Y	Y	N	N

Create a ZBFW Zone

Resource URI

Verb	URI
POST	/api/v1/zbfw-svc/zones

Example

JSON Request

```
POST /api/v1/zbfw-svc/zones
```

```
Accept: application/json
Content-type: application/json
```

```
{
  "zone-name": "inside",
  "-list": { "tunnel0", "gig0" }
}
```

JSON Response

```
201 Created
Location: http://host/api/v1/zbfw-svc/zone/inside
```

ZBFW Zone Resource

History

Release	Modification
IOS XE 3.10	Introduced for the CSR1000V platform
IOS XE 3.14	Introduced for ASR1001-X and ASR1002-X platforms

Properties

Property	Type	Required for POST and PUT	Description
zone-name	string	Mandatory	Name of a zone. "self" and "default" are not allowed.
interface-list	array of string	Mandatory	One or more s that belong to the zone.

JSON Representation

```
{
  "kind": "object#zbfw-zone",
  "zone-name": "{string}",
  "interface-list": [{"string"}]
}
```

Modify a ZBFW Zone

Resource URI

Verb	URI
PUT	/api/v1/zbfw-svc/zones/inside

Example

JSON Request

```
PUT /api/v1/zbfw-svc/zones/inside
Content-type: application/json
Accept: application/json
```

```
{
  "zone-name": "inside",
  "-list": { "gig0" }
}
```

JSON Response

```
204 No Content
```

Retrieve a ZBFW Zone

Resource URI

Verb	URI
GET	/api/v1/zbfw-svc/zones/{zone-name}

Example

JSON Request

```
GET /api/v1/zbfw-svc/zones/inside
Accept: application/json
```

JSON Response

200 OK

Content-type: application/json

```
{
  "kind": "object#zbfw-zone",
  "zone-name": "inside",
  "-list": { "tunnel0", "gig0" }
}
```

Retrieve All ZBFW Zones

Resource URI

Verb	URI
GET	/api/v1/zbfw-svc/zones

Properties for Retrieve All

Property	Type	Required for POST and PUT	Description
kind	string	Not applicable	Must be collection#zbfw-zone
items	array	Mandatory	Collection of zbfw zones.

JSON Representation

```
{
  "kind": "collection#zbfw-zone",
  "items": { { zbfw-zone JSON object }+ }
}
```

Example**JSON Request**

```
GET /api/v1/zbfw-svc/zones
Accept: application/json
```

JSON Response

200 OK

Content-type: application/json

```
{
  "kind": "collection#zbfw-zone",
  "items": [
    {
      "kind": "object#zbfw-zone",
      "zone-name": "inside",

```

```

        "-list": { "tunnel0", "gig0" }
      },
      {
        "kind": "object#zbfw-zone",
        "zone-name": "outside",
        "-list": { "gig1" }
      }
    ]
  }

```

Delete a ZBFW Zone

Resource URI

Verb	URI
DELETE	/api/v1/zbfw-svc/zones/{zone-name}

Example

JSON Request

```

DELETE /api/v1/zbfw-svc/zones/inside
Accept: application/json

```

JSON Response

```

204 No Content

```

Create a ZBFW Filter

Resource URI

Verb	URI
POST	/api/v1/zbfw-svc/filters

Example

JSON Request

```

POST /api/v1/zbfw-svc/filters

Accept: application/json
Content-type: application/json

```

```

{
  "filter-name": "engFilter",
  "match-type": "any",
  "match-list": [ {"acl": "eng1Acl"},
                  {"protocol": "egp"},
                  {"acl": "eng2Acl"}
                ]
}

```

}

JSON Response

201 Created

Location: http://host/api/v1/zb主w-svc/filter/engFilter

ZBFW Filter Resource

History

Release	Modification
IOS XE 3.10	Introduced for the CSR1000V platform
IOS XE 3.14	Introduced for ASR1001-X and ASR1002-X platforms

Properties

Property	Type	Required for POST and PUT	Description
kind	string	Not applicable	Must be object#zb主w-filter
filter	string	Mandatory	“class-default” or a name to describe the traffic (the IOS class-map name). The name cannot be modified once it is created.
match-type	string	Optional	“Any” or “All”. “Any”(match any of the traffic criteria) is the default. “Any” refers to the OR operator, and “All” refers to the AND operator.
match-acl-list	array of string	Optional, if the traffic protocol-list attribute is set	0 or n types of ACL traffic we want to monitor: one or n acl-id that were configured using the ACL resource.
match-protocol-list	array of string	Optional if the traffic ACL-list attribute is set	0 to n traffic protocols to monitor. All protocols supported by the CLI are supported.

JSON Representation (IOS Class-map with “type inspect” by Default)

```
{
  "kind": "object#zb主w-filter",
  "filter-name": "{string}",
  "match-type": "{string}",
  "match-acl-list": "{string}",
  "match-protocol-list": "{string}"
}
```

Modify a ZBFW Filter

Example

JSON Request

```
PUT /api/v1/zb主fw-svc/filters/engFilter
Content-type: application/json
Accept: application/json
```

```
{
  "filter-name": "engFilter",
  "match-type": "any",
  "match-list": [
    { "acl": "dosAcl" },
    { "protocol": "egp" },
    { "acl": "dos2Acl" }
  ]
}
```

JSON Response

```
204 No Content
```

Retrieve a ZBFW Filter

Resource URI

Verb	URI
GET	/api/v1/zb主fw-svc/filters/{filter-name}

Example

JSON Request

```
GET /api/v1/zb主fw-svc/filter/engFilter
Accept: application/json
```

JSON Response

```
200 OK
```

```
Content-type: application/json
```

```
{
  "kind": "object#zb主fw-filter",
  "filter-name": "engFilter",
  "match-type": "any",
  "match-list": [{"acl": "dosAcl"}, {"protocol": "egp"}]
}
```


Retrieve All ZBFW Filters

Resource URI

Verb	URI
GET	/api/v1/zbfw-svc/filters

Properties for Retrieve All

Property	Type	Required for POST and PUT	Description
kind	string	Mandatory	Must be collection#zbfw-filter
items	array	Mandatory	Collection of zone-base-firewall filters.

JSON Representation

```
{
  "kind": "collection#zbfw-filter",
  "items": [ { zbfw-filter JSON object } ]
}
```

Example

JSON Request

```
GET /api/v1/zbfw-svc/filters
Accept: application/json
```

JSON Response

```
200 OK

Content-type: application/json

{
  "kind": "collection#zbfw-filter",
  "items": [
    {
      "kind": "object#zbfw-filter",
      "filter-name": "engFilter",
      "match-type": "any",
      "match-acl-list": [{"dosAcl"}],
      "match-list": [{"protocol": "egp"}]
    },
    {
      "kind": "object#zbfw-filter",
      "filter-name": "engFilter",
      "match-type": "any",
      "match-list": [{"protocol": "ip"}]
    }
  ]
}
```

Delete a ZBFW Filter

Resource URI

Verb	URI
DELETE	/api/v1/zbfw-svc/filters/{filter-name}

JSON Request

DELETE /api/v1/zbfw-svc/filter/engFilter
 Accept: application/json

JSON Response

204 No Content

ZBFW Policy Resource

History

Release	Modification
IOS XE 3.10	Introduced for the CSR1000V platform
IOS XE 3.14	Introduced for ASR1001-X and ASR1002-X platforms

Properties

Property	Type	Required for POST and PUT	Description
kind	string	Mandatory	Must be object#zbfw-policy
name	string	Mandatory	Name of the firewall inspection policy resource (the IOS zone-pair security name).
description	string	Optional	FW Description
source-zone	string	Mandatory	Source zone name. “self” and “default” are not allowed.
destination-zone	string	Mandatory	Destination zone name. “self” and “default” are not allowed.
{rule-list}	array	Mandatory	List of pairs of filter name and action.
filter-name	string	Mandatory	“class-default” or a filter name.
filter-action	string	Optional	Default is “drop”. “inspect”, “drop”, “drop-log”, “pass”, and “pass-log”

JSON Representation of ZBFW Policy

```
{
  "kind": "object#zbfw-policy"
  "name": "{string}",
  "description": "{string}",
  "source-zone": "{string}",
  "destination-zone": "{string}",
  "rule-list": [
    {
      "filter-name": "{string}",
      "filter-action": "{string}"
    }
  ]
}
```

Modify a Firewall Policy

Resource URI

Verb	URI
PUT	/api/v1/zbfw-svc/policies/{policy-id}

Example

JSON Request

PUT /api/v1/zbfw-svc/policies/zone_pair_in_to_out

Content-type: application/json

Accept: application/json

```
{
  "name": "zone_pair_in_to_out",
  "description": "Inside to Outside firewall",
  "source-zone": "inside",
  "destination-zone": "outside",
  "rule-list": [
    {
      "filter-name": " class_map_in_to_out",
      "filter-action": "inspect",
    },
    {
      "filter-name": " class_map_in_to_out2",
      "filter-action": "inspect"
    }
  ]
}
```

JSON Response

204 No Content

Create a Firewall Policy

Resource URI

Verb	URI
POST	/api/v1/zbfw-svc/policies

Example

JSON Request

```
POST /api/v1/zbfw-svc/policies
```

```
Content-type: application/json
```

```
Accept: application/json
```

```
{
  "name": "zonePair_in2out",
  "description": "",
  "source-zone": "inside",
  "destination-zone": "outside",
  "rule-list": [
    {
      "filter-name": "class_map_in_to_out",
      "filter-action": "inspect"
    }
  ]
}
```

JSON Response

```
201 Created
```

```
Location: http://host/api/v1/zbfw-svc/policy/zonePair_in2out
```

Retrieve a Firewall Policy

Resource URI

Verb	URI
GET	/api/v1/zbfw-svc/policies/{policy-id}

Example

JSON Request

```
GET /api/v1/zbfw-svc/policies/zone_pair_in_to_out
```

```
Accept: application/json
```

JSON Response

200 OK

Content-type: application/json

```
{
  "kind": "object#zone-pair-fw-policy",
  "policy-name": "zone_pair_in_to_out",
  "description": "",
  "sourcename": "inside",
  "rule-list": [
    {
      "filter-name": " class_map_in_to_out",
      "filter-action": "inspect"
    },
    {
      "filter-name": " class_map_in_to_out2",
      "filter-action": "inspect"
    }
  ]
}
```

Retrieve All Firewall Policies

Resource URI

Verb	URI
GET	/api/v1/zbfw-svc/policies

Properties for Retrieve All

Property	Type	Required for POST and PUT	Description
kind	string	Mandatory	Must be collection#zbfw-policy
items	array	Mandatory	Collection of zone base firewall policies.

JSON Representation

```
{
  "kind": "collection#zbfw-policy",
  "items": [ { zbfw-policy JSON object } ]
}
```

Example**JSON Request**

```
GET /api/v1/zbfw-svc/policies
Accept: application/json
```

JSON Response

200 OK

Content-type: application/json

Accept: application/json

```

{
  "kind": "collection#zbfw-policy"
  "items": [
    {
      "kind": "object#zbfw-policy",
      "name": "zone_pair_in_to_out",
      "source-zone": "inside",
      "destination-zone": "outside",
      "rule-list": [
        {
          "filter-name": "class_map_in_to_out",
          "filter-action": "inspect"
        }
      ]
    },
    {
      "kind": "object#zbfw-policy",
      "name": "myFirewallPolicy",
      "source-zone": "inside",
      "destination-zone": "outside",
      "rule-list": [
        {
          "filter-name": "myClassMap1",
          "filter-action": "inspect"
        },
        {
          "filter-name": "myClassMap2",
          "filter-action": "inspect"
        }
      ]
    }
  ]
}

```

Delete a Firewall Policy

Resource URI

Verb	URI
DELETE	/api/v1/zbfw-svc/policies/{policy-id}

Example**JSON Request**

DELETE /api/v1/zbfw-svc/policy/zone_pair_in_to_out

Accept: application/json

JSON Response

204 No Content

Firewall Session Collection Resource

History

Release	Modification
IOS XE 3.10	Introduced for the CSR1000V platform
IOS XE 3.14	Introduced for ASR1001-X and ASR1002-X platforms

Properties

Property	Type	Required for POST and PUT	Description
kind	string	Not applicable	object#firewall-session
policy-id	string	Not applicable	Name of the policy
source-ip	ipaddress	Not applicable	Source IP address
destination-ip	ipaddress	Not applicable	Destination IP address
traffic-protocol	string	Not applicable	IP protocol
source-protocol-port	number	Not applicable	Source port of the protocol
destination-protocol-port	number	Not applicable	Destination port of the protocol

JSON Representation

```
{
  "kind": "collection#firewall-session",
  "items": [
    {
      "kind": "object#firewall-session",
      "policy-id": "{string}",
      "source-ip": "{ipaddress}",
      "destination-ip": "{ipaddress}",
      "traffic-protocol": "{string}",
      "source-protocol-port": {number},
      "destination-protocol-port": {number}
    }
  ]
}
```

Retrieve All Firewall “Sessions”

Resource URI

Verb	URI
GET	/api/v1/zbfw-svc/active-sessions

Example

JSON Request

```
GET /api/v1/zbfw-svc/active-sessions
Accept: application/json
```

JSON Response

```
204 No Content
```

```
Content-type: application/json
```

```
{
  "kind": "collection#zbfw-session",
  "items": [
    {
      "kind": "object#zbfw-session",
      "policy-id": "in-to-out",
      "source-ip": "36.1.1.4",
      "destination-ip": "37.1.1.2",
      "traffic-protocol": "udp",
      "source-protocol-port": 63,
      "destination-protocol-port": 63
    },
    {
      "kind": "object#zbfw-session",
      "policy-id": "in-to-out",
      "source-ip": "36.1.1.5",
      "destination-ip": "37.1.1.2",
      "traffic-protocol": "udp",
      "source-protocol-port": 63,
      "destination-protocol-port": 63
    }
  ]
}
```

Set Firewall High-Speed Logger Resource

The high-speed logger will log the alert messages by default, which include packet drops.

History

Release	Modification
IOS XE 3.10	Introduced for the CSR1000V platform
IOS XE 3.14	Introduced for ASR1001-X and ASR1002-X platforms

Properties

Property	Type	Required for POST and PUT	Description
kind	string	Not applicable	Object#firewall-log
enable	boolean	Mandatory	“true” to enable the logging, or “false” to disable it.
dest-address	ipaddress	Mandatory	IP address in x.x.x.x format of where the log should be redirected to.
dest-udp-port	number	Mandatory	Destination UDP port

JSON Representation

```
{
  "kind": "object#firewall-log",
  "enable": "{string}",
  "dest-ip-address": {ipaddress},
  "dest-udp-port": {number}
}
```

Retrieve Firewall Log Server Parameters

Resource URI

Verb	URI
GET	/api/v1/zbfw-svc /log

Example

JSON Request

```
GET /api/v1/zbfw-svc/log
Accept: application/json
```

JSON Response

204 No Content

```
Content-type: application/json

{
  "kind": "object#firewall-log",
  "enable": true,
  "dest-ip-address": "25.25.25.25",
  "dest-udp-port": 25
}
```

Modify the Firewall Log Server

Resource URI

Verb	URI
PUT	/api/v1/zbfw-svc /log

Example**JSON Request**

PUT /api/v1/zbfw-svc/log

```
Content-type: application/json
Accept: application/json
```

```
{
  "enable": false,
  "dest-ip-address": 25.25.25.25,
  "dest-udp-port": 26
}
```

JSON Response

204 No Content

Firewall Statistics (Global Count) Resource

History

Release	Modification
IOS XE 3.10	Introduced for the CSR1000V platform
IOS XE 3.14	Introduced for ASR1001-X and ASR1002-X platforms

Properties

Property	Type	Required for POST and PUT	Description
kind	object	Not applicable	collection#firewall-statistics
drop-count	string	Not applicable	
firewall-back-pressure packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall back pressure packet and byte counts.
firewall-invalid-zone packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall invalid zone packet and byte counts.
firewall-l4-insp packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall layer 4 inspection packet and byte counts.
firewall-no-forwarding-zone packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall no forwarding zone packet and byte counts.
firewall-non-session packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall non-session packet and byte counts.
firewall-policy packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall policy packet and byte counts.
firewall-L4 packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall layer 4 packet and byte counts.
firewall-L7 packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall layer 7 packet and byte counts.
firewall-not-initiator packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall not-initiator packet and byte counts.
firewall-no-new-session packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall no new session packet and byte counts.

Property	Type	Required for POST and PUT	Description
firewall-syn-cookie-max-dst packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall TCP SYN cookie maximum destination packet and byte counts.
firewall-syn-cookie packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall TCP SYN cookie packet and byte counts.
firewall-AR-standby packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall asymmetric routing standby packet and byte counts.
firewall-not-from-init packet count byte count	number	Not applicable	(sub-property of drop-count) Firewall not from initiator packet and byte counts.
items	array	Not applicable	Array of objects that define zone-based firewall session statistics. Each object includes: <ul style="list-style-type: none"> • kind • policy-id • byte-stats • packet-stats
kind	string	Not applicable	object#zbfw-session-stats
policy-id	string	Not applicable	Name of the policy
byte-stats	object	Not applicable	Statistics in bytes
source-ip	ipaddress	Not applicable	(sub-property of byte-stats) Source IP address
destination-ip	ipaddress	Not applicable	(sub-property of byte-stats) Destination IP address
traffic-protocol	string	Not applicable	(sub-property of byte-stats) Traffic protocol
source-protocol-port	number	Not applicable	(sub-property of byte-stats) Source protocol port
destination-protocol-port	number	Not applicable	(sub-property of byte-stats) Destination protocol port
tx-byte-count	number	Not applicable	(sub-property of byte-stats) Transmit byte count

Property	Type	Required for POST and PUT	Description
rx-byte-count	number	Not applicable	(sub-property of byte-stats) Receive byte count
packet-stats	object	Not applicable	Statistics in packets
traffic-protocol	string	Not applicable	(sub-property of packet-stats) Traffic protocol
packet-count	string	Not applicable	(sub-property of packet-stats) Packet count

JSON Representation

```
{
  "kind": "collection#firewall-statistics",
  "drop-count": {
    {
      "firewall-back-pressure":
        {"packet-count": {number}, "byte-count": {number}}
    },
    {
      "firewall-invalid-zone":
        {"packet-count": {number}, "byte-count": {number}}
    },
    {
      "firewall-l4-insp":
        {"packet-count": {number}, "byte-count": {number}}
    },
    {
      "firewall-no-forwarding-zone":
        {"packet-count": {number}, "byte-count": {number}}
    },
    {
      "firewall-non-session":
        {"packet-count": {number}, "byte-count": {number}}
    },
    {
      "firewall-policy":
        {"packet-count": {number}, "byte-count": {number}}
    },
    {
      "firewall-L4":
        {"packet-count": {number}, "byte-count": {number}}
    },
    {
      "firewall-L7":
        {"packet-count": {number}, "byte-count": {number}}
    },
    {
      "firewall-not-initiator":
        {"packet-count": {number}, "byte-count": {number}}
    },
    {
      "firewall-no-new-session":
        {"packet-count": {number}, "byte-count": {number}}
    },
    {

```

```

    "firewall-syn-cookie-max-dst":
      {"packet-count":{number},"byte-count": {number}}
  },
  {
    "firewall-syn-cookie":
      {"packet-count":{number},"byte-count": {number}}
  },
  {
    "firewall-AR-standby":
      {"packet-count":{number},"byte-count": {number}}
  },
  {
    "firewall-not-from-init":
      {"packet-count":{number},"byte-count": {number}}
  },
},
"items": [
  {
    "kind": "object#zbfw-session-stats",
    "policy-id": "{string}",
    "byte-stats": [
      {
        "source-ip": "{ipaddress}",
        "destination-ip": "{ipaddress}",
        "traffic-protocol": "{string}",
        "source-protocol-port": {number},
        "destination-protocol-port":{number},
        "tx-byte-count": {number},
        "rx-byte-count": {number}
      }
    ],
    "packet-stats": [
      {
        "traffic-protocol": "{string}",
        "packet-count": {number}
      }
    ]
  }
]
}

```

Retrieve Firewall Statistics

Resource URI

Verb	URI
GET	/api/v1/zbfw-svc/statistics

Example

JSON Request

```

GET /api/v1/zbfw-svc/statistics
Accept: application/json

```

JSON Response

200 OK

Content-type: application/json

```

{
  "kind": "collection#firewall-statistics",
  "drop-count": {
    {
      "firewall-back-pressure":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-invalid-zone":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-l4-insp":
        {"packet-count":7,"byte-count": 616}
    },
    {
      "firewall-no-forwarding-zone":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-non-session":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-policy":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-L4":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-L7":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-not-initiator":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-no-new-session":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-syn-cookie-max-dst":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-syn-cookie":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-AR-standby":
        {"packet-count":0,"byte-count": 0}
    },
    {
      "firewall-not-from-init":
        {"packet-count":0,"byte-count": 0}
    }
  }
}

```

```

    },
  },
  "items": [
    {
      "kind": "object#zbfw-session-stats",
      "policy-id": "in-to-out",
      "byte-stats": [
        {
          "source-ip": "36.1.1.4",
          "destination-ip": "37.1.1.2"
          "traffic-protocol": "udp"
          "source-protocol-port": 63,
          "destination-protocol-port": 63,
          "tx-byte-count": 54,
          "rx-byte-count": 0
        }
      ],
      "packet-stats": [
        {
          "traffic-protocol": "udp",
          "packet-count": 5
        }
      ]
    }
  ]
}

```

Clear Firewall Statistics

Example

JSON Request

```

POST /api/v1/zbfw-svc/statistics
Accept: application/json
{
  "action": "clear"
}

```

JSON Response

```

204 No Content

```