cSRX validation on SUSE Rancher: RKE2

v1.3

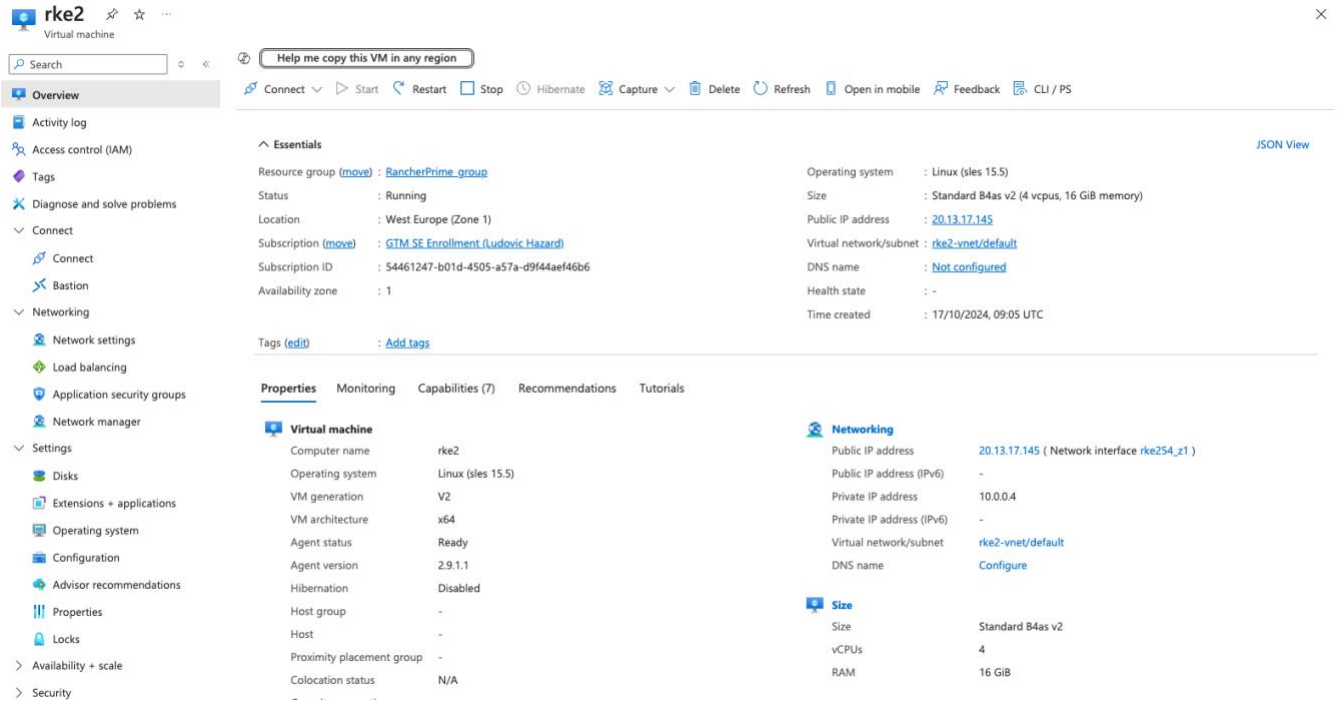
Content

Introduction

This document details the validation activities performed with cSRX (junos versions 21.1R3.11 and 24.2R1.17) on SUSE Rancher: RKE2 (v1.30.5+rke2r1).

The objectives of this validation is to confirm the expected behavior of basic NGFW features delivered by the Juniper cSRX VNF on SUSE Rancher: KE2. The L3/L4 Firewall rules are configured on the cSRX that acts as the default gateway for 2 ubuntu pods located on different vnets (network-attachment-definition used macvlan in the scenario).

The single node SUSE Rancher: RKE2 used durign the validation activities is hosted on Azure:



The details about the SUSE Rancher: RKE2 version used for the validation activities are listed below:

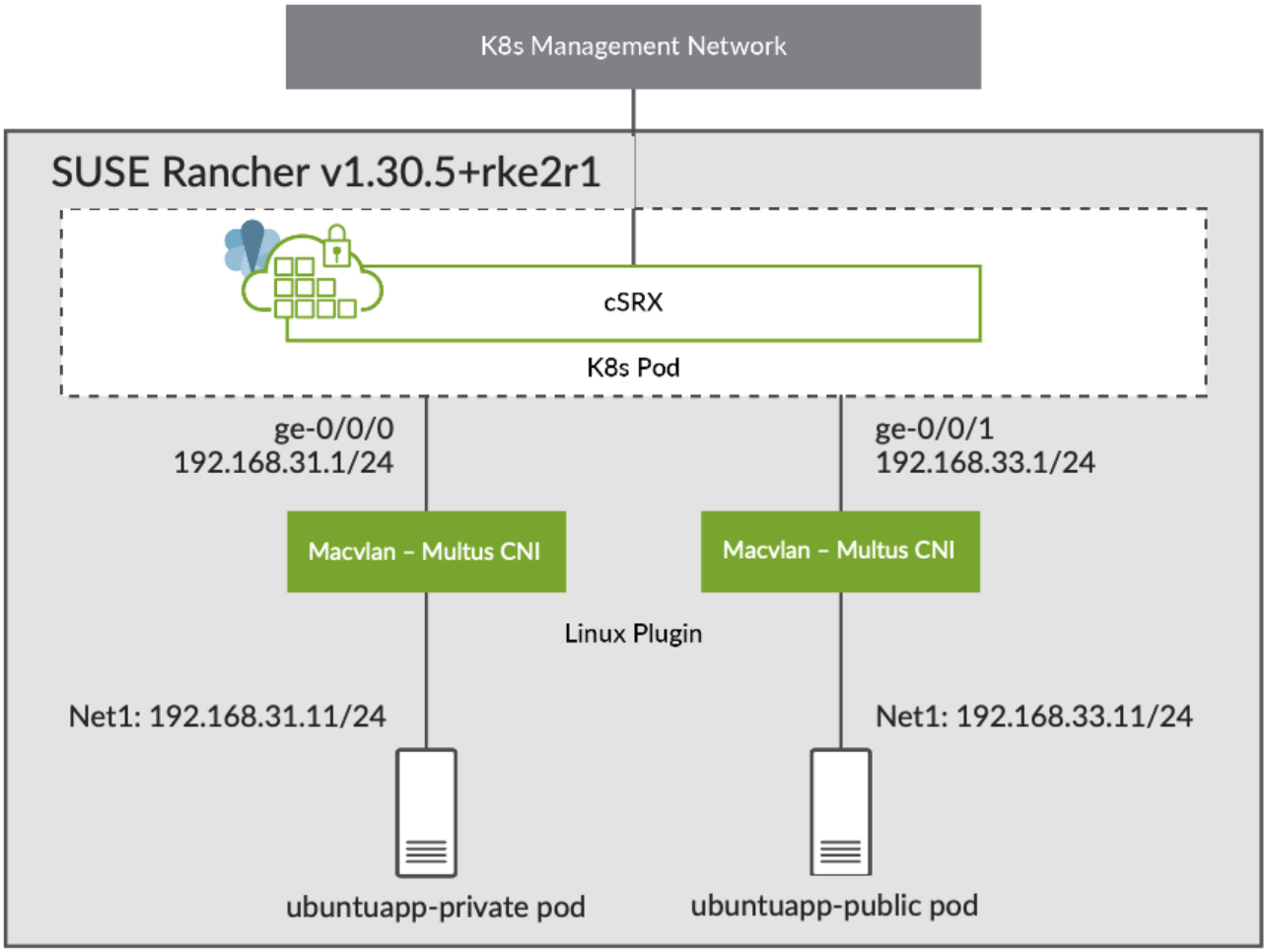
```
azureuser@rke2:~/validation> kubectl version
Client Version: v1.30.5+rke2r1
Kustomize Version: v5.0.4-0.20230601165947-6ce0bf390ce3
Server Version: v1.30.5+rke2r1
azureuser@rke2:~/validation>
```

Validation Scenario

The “k8s internal networks” scenario (described on the documentation available thru the link below) has been used for the validation activities:

https://www.juniper.net/documentation/us/en/software/csrx/csrx-consolidated-deployment-guide/csrx-kubernetes-deployment/topics/task/connecting-csrx-internal-network-k8s.html

This figure details the validation architecture inside the SUSE Rancher: RKE2 single node cluster:

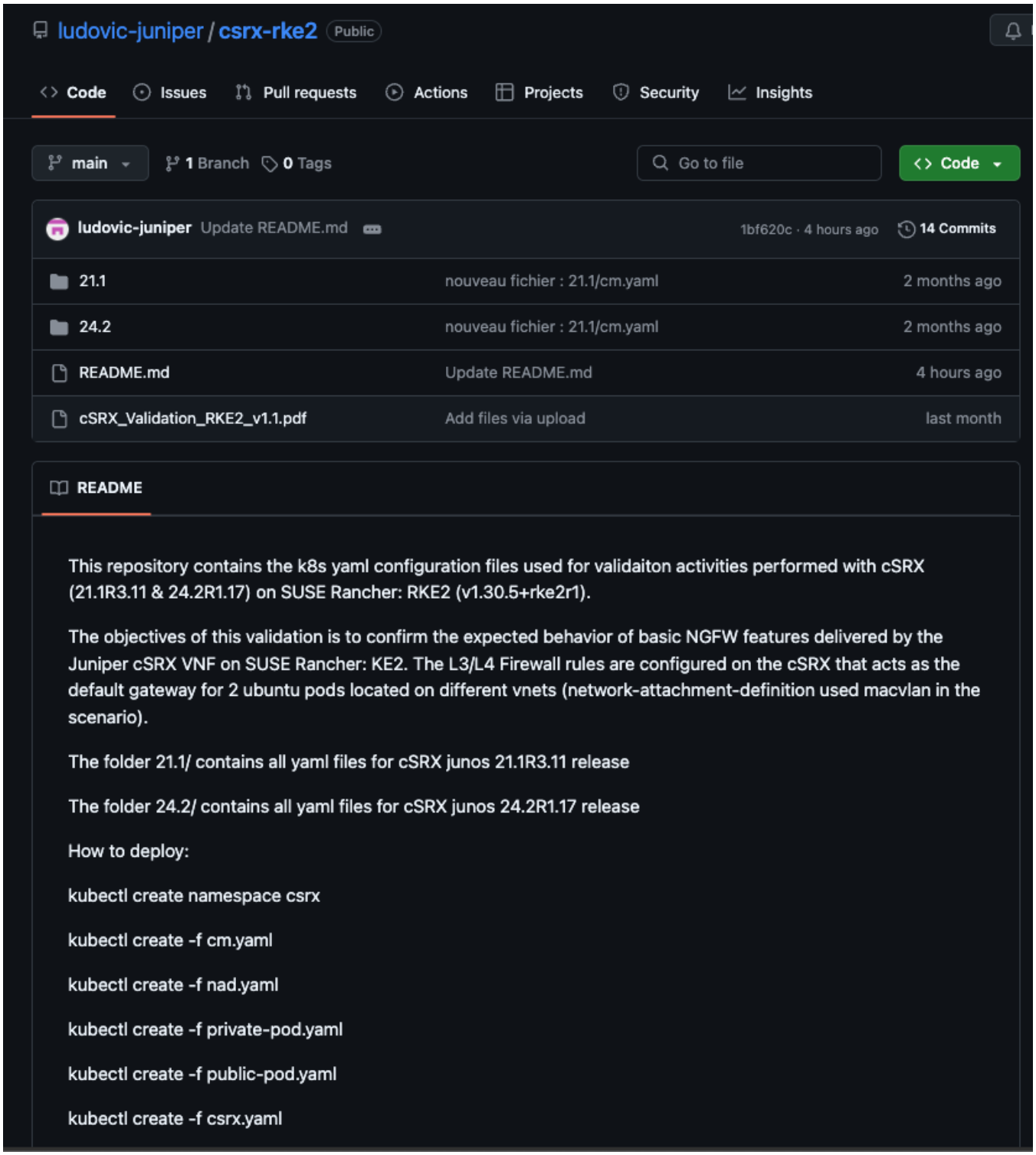


The same validation scenario has been used for cSRX validation on RedHat OpenShift:
Juniper cSRX validation on RedHat OpenShift

For more information about Juniper CNFs validation on RedHat OpenShift:
https://catalog.redhat.com/search?gs&q=juniper&searchType=software

Environment details

The configuration files used for the validation are available at:
https://github.com/ludovic-juniper/csrx-rke2



The k8s namespace cSRX contains 3 pods and 2 network-attachment-definitions using macvlan to connect cSRX with ubuntu pods as detailled in the diagram above:

CSRX 21.1R3.11

```
azureuser@rke2:~> kubectl get pods -n csrx -o wide
NAME                READY   STATUS    RESTARTS      AGE   IP           NODE   NOMINATED NODE   READINESS
GATES
csrx                1/1     Running   1 (12m ago)   39d   10.42.0.22   rke2   <none>           <none>
ubuntuapp-private   1/1     Running   1 (12m ago)   39d   10.42.0.25   rke2   <none>           <none>
ubuntuapp-public    1/1     Running   2 (10m ago)   39d   10.42.0.24   rke2   <none>           <none>
azureuser@rke2:~>
```

```
azureuser@rke2:~/validation> kubectl describe pods -n csrx
Name:             csrx
Namespace:        csrx
Priority:         0
Service Account:  default
Node:             rke2/10.0.0.4
Start Time:       Thu, 17 Oct 2024 09:21:40 +0000
Labels:           <none>
Annotations:      cni.projectcalico.org/containerID:
aa9c220dfaa3903f98ba4873b6d116b3d28f330487ac6647e22859a36d39688d
                  cni.projectcalico.org/podIP: 10.42.0.22/32
                  cni.projectcalico.org/podIPs: 10.42.0.22/32
                  k8s.v1.cni.cncf.io/network-status:
                    [{
                        "name": "csrx/network-conf-1",
                        "interface": "net1",
                        "ips": [
                            "192.168.31.0"
                        ],
                        "mac": "a6:71:9c:ac:18:2a",
                        "dns": {},
                        "gateway": [
                            "\u003cnil\u003e"
                        ]
                    },{
                        "name": "csrx/network-conf-2",
                        "interface": "net2",
                        "ips": [
                            "192.168.33.0"
                        ],
                        "mac": "c2:00:9c:40:2f:2d",
                        "dns": {},
                        "gateway": [
                            "\u003cnil\u003e"
                        ]
                    }]
                  k8s.v1.cni.cncf.io/networks: [ { "name": "network-conf-1" }, { "name": "network-conf-
2" } ]
Status:           Running
IP:               10.42.0.22
IPs:
  IP:  10.42.0.22
Containers:
  csrx:
    Container ID:   containerd://61da5a52fa8613720c658fe1fd8b1a7b810ca1ef61aeca4e48bef6bc2d20d853
    Image:          quay.io/juniper-128t/csrx:21.1R3.11
```

```
    Image ID:       quay.io/juniper-
128t/csrx@sha256:34fb717a2ee84fd853790273967f966cf2028fb3889afc820cc80607e1c23f55
    Port:           <none>
    Host Port:      <none>
    State:          Running
      Started:      Mon, 25 Nov 2024 10:48:12 +0000
    Last State:     Terminated
      Reason:       Unknown
      Exit Code:    255
      Started:      Thu, 17 Oct 2024 09:22:02 +0000
      Finished:     Mon, 25 Nov 2024 10:47:26 +0000
    Ready:          True
    Restart Count:  1
    Environment:
      CSRX_ROOT_PASSWORD:   lab123
      CSRX_SIZE:            large
      CSRX_HUGEPAGES:       no
      CSRX_PACKET_DRIVER:   interrupt
      CSRX_AUTO_ASSIGN_IP:  yes
      CSRX_FORWARD_MODE:    routing
      CSRX_LICENSE_FILE:    /var/jail/.csrx_license
      CSRX_JUNOS_CONFIG:    var/jail/csrx_config
    Mounts:
      /var/jail from config (rw)
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-fqgzn (ro)
Conditions:
  Type                        Status
  PodReadyToStartContainers   True
  Initialized                 True
  Ready                       True
  ContainersReady             True
  PodScheduled                True
Volumes:
  config:
    Type:      ConfigMap (a volume populated by a ConfigMap)
    Name:      csrx-config-map
    Optional:  false
  kube-api-access-fqgzn:
    Type:                     Projected (a volume that contains injected data from multiple sources)
    TokenExpirationSeconds:   3607
    ConfigMapName:            kube-root-ca.crt
    ConfigMapOptional:        <nil>
    DownwardAPI:              true
QoS Class:                    BestEffort
Node-Selectors:               <none>
Tolerations:                  node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                              node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events:                       <none>


Name:             ubuntuapp-private
Namespace:        csrx
Priority:         0
Service Account:  default
Node:             rke2/10.0.0.4
Start Time:       Thu, 17 Oct 2024 09:20:44 +0000
Labels:           app=ubuntuapp
                  zone=private
Annotations:      cni.projectcalico.org/containerID:
75507222a89e7dc70d8c3d62a41cd6664b73d2502d401550c0addfcd1f80c537
                  cni.projectcalico.org/podIP: 10.42.0.25/32
                  cni.projectcalico.org/podIPs: 10.42.0.25/32
                  k8s.v1.cni.cncf.io/network-status:
                    [{
                        "name": "csrx/network-conf-1",
                        "interface": "net1",
                        "ips": [
                            "192.168.31.0"
                        ],
                        "mac": "16:3d:4e:14:0d:a0",
                        "dns": {},
```

```
                        "gateway": [
                            "\u003cnil\u003e"
                        ]
                    }]
                  k8s.v1.cni.cncf.io/networks: [{ "name": "network-conf-1" }]
                  k8s.v1.cni.cncf.io/networks-status:
                    [{
                        "name": "network-conf-1",
                        "interface": "net1",
                        "ips": [
                            "192.168.31.11"
                        ],
                        "mac": "22:2f:60:a5:ff:01",
                        "dns": {}
                    }]
Status:           Running
IP:               10.42.0.25
IPs:
  IP:  10.42.0.25
Containers:
  ubuntuapp:
    Container ID:  containerd://f37563adf91322bc2a4ae4b9e3868156fe9912fd3a37b0d6184edfe6a68e8877
    Image:         ubuntu-upstart
    Image ID:      sha256:caf860ff39ff6acbecc1e01d86d0a22e6a59b5fb10dc624e2c638161fc7dfa37
    Port:          <none>
    Host Port:     <none>
    Command:
      sh
      -c
      ifconfig net1 192.168.31.11/24;route add -net 192.168.33.0/24 gw 192.168.31.1;mount
/sys/fs/selinux -o remount,ro; apt install iperf; apt install ethtool; ethtool -K net1 tx off; sleep 40;
iperf -c 192.168.33.11 -t 300;sleep 100d
    State:          Running
      Started:      Mon, 25 Nov 2024 10:48:14 +0000
    Last State:     Terminated
      Reason:       Unknown
      Exit Code:    255
      Started:      Thu, 17 Oct 2024 09:20:52 +0000
      Finished:     Mon, 25 Nov 2024 10:47:26 +0000
    Ready:          True
    Restart Count:  1
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-qsnj2 (ro)
Conditions:
  Type                        Status
  PodReadyToStartContainers   True
  Initialized                 True
  Ready                       True
  ContainersReady             True
  PodScheduled                True
Volumes:
  kube-api-access-qsnj2:
    Type:                    Projected (a volume that contains injected data from multiple sources)
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
    DownwardAPI:             true
QoS Class:                   BestEffort
Node-Selectors:              <none>
Tolerations:                 node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events:                      <none>


Name:             ubuntuapp-public
Namespace:        csrx
Priority:         0
Service Account:  default
Node:             rke2/10.0.0.4
Start Time:       Thu, 17 Oct 2024 09:20:49 +0000
```

```
Labels:           app=ubuntuapp
                  zone=private
Annotations:      cni.projectcalico.org/containerID:
a9c2ffe4dcd06ab3f1d79c0a3536abaa2b2faad19b1569103d94dcbc2364bacc
                  cni.projectcalico.org/podIP: 10.42.0.24/32
                  cni.projectcalico.org/podIPs: 10.42.0.24/32
                  k8s.v1.cni.cncf.io/network-status:
                    [{
                        "name": "csrx/network-conf-2",
                        "interface": "net1",
                        "ips": [
                            "192.168.33.0"
                        ],
                        "mac": "ca:55:47:78:6f:8f",
                        "dns": {},
                        "gateway": [
                            "\u003cnil\u003e"
                        ]
                    }]
                  k8s.v1.cni.cncf.io/networks: [{ "name": "network-conf-2" }]
                  k8s.v1.cni.cncf.io/networks-status:
                    [{
                        "name": "network-conf-2",
                        "interface": "net1",
                        "ips": [
                            "192.168.33.11"
                        ],
                        "mac": "22:2f:60:a5:ff:02",
                        "dns": {}
                    }]
Status:           Running
IP:               10.42.0.24
IPs:
  IP:  10.42.0.24
Containers:
  ubuntuapp:
    Container ID:  containerd://00364a3940cf5f4c1010d831d130c047c95b9646da5d399e9e70628162b89240
    Image:         ubuntu-upstart
    Image ID:      sha256:caf860ff39ff6acbecc1e01d86d0a22e6a59b5fb10dc624e2c638161fc7dfa37
    Port:          <none>
    Host Port:     <none>
    Command:
      sh
      -c
      ifconfig net1 192.168.33.11/24;route add -net 192.168.31.0/24 gw 192.168.33.1;mount
/sys/fs/selinux -o remount,ro; apt install iperf; apt install ethtool; ethtool -K net1 tx off;iperf -s
    State:          Running
      Started:      Mon, 25 Nov 2024 11:25:05 +0000
    Last State:     Terminated
      Reason:       Error
      Exit Code:    137
      Started:      Mon, 25 Nov 2024 10:48:52 +0000
      Finished:     Mon, 25 Nov 2024 11:25:03 +0000
    Ready:          True
    Restart Count:  3
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-cbl2b (ro)
Conditions:
  Type                        Status
  PodReadyToStartContainers   True
  Initialized                 True
  Ready                       True
  ContainersReady             True
  PodScheduled                True
Volumes:
  kube-api-access-cbl2b:
    Type:                    Projected (a volume that contains injected data from multiple sources)
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
```

```
    DownwardAPI:             true
QoS Class:                   BestEffort
Node-Selectors:              <none>
Tolerations:                 node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events:                      <none>
azureuser@rke2:~/validation>
```

```
azureuser@rke2:~/validation> kubectl get network-attachment-definition -n csrx
NAME             AGE
network-conf-1   39d
network-conf-2   39d
azureuser@rke2:~/validation>
```

```
azureuser@rke2:~/validation> kubectl describe network-attachment-definition -n csrx
Name:         network-conf-1
Namespace:    csrx
Labels:       <none>
Annotations:  <none>
API Version:  k8s.cni.cncf.io/v1
Kind:         NetworkAttachmentDefinition
Metadata:
  Creation Timestamp:  2024-10-17T09:20:39Z
  Generation:          1
  Resource Version:    2727
  UID:                 9809b0f6-fc6f-4ce9-bd3a-8b931a30f408
Spec:
  Config:  { "cniVersion": "0.3.0", "type": "bridge", "master": "eno2", "promiscMode": true, "ipam": {
"type": "static", "addresses": [ { "address": "192.168.31.0/24", "gateway": "192.168.31.1" } ],
"routes": [ { "dst": "0.0.0.0/0" } ] } }
Events:    <none>


Name:         network-conf-2
Namespace:    csrx
Labels:       <none>
Annotations:  <none>
API Version:  k8s.cni.cncf.io/v1
Kind:         NetworkAttachmentDefinition
Metadata:
  Creation Timestamp:  2024-10-17T09:20:39Z
  Generation:          1
  Resource Version:    2728
  UID:                 d4f2ad8d-8d65-4507-80f2-03ad6d49e91a
Spec:
  Config:  { "cniVersion": "0.3.0", "type": "bridge", "master": "eno3", "promiscMode": true, "ipam": {
"type": "static", "addresses": [ { "address": "192.168.33.0/24", "gateway": "192.168.33.1" } ],
"routes": [ { "dst": "0.0.0.0/0" } ] } }
Events:    <none>
azureuser@rke2:~/validation>
```

cSRX Configuration :

```
root@csrx> show configuration | display set
set version 20211201.145818_builder.r1226460
set interfaces ge-0/0/0 unit 0 family inet address 192.168.31.1/24
set interfaces ge-0/0/1 unit 0 family inet address 192.168.33.1/24
set security policies from-zone trust to-zone untrust policy permit-ping-iperf match source-address any
set security policies from-zone trust to-zone untrust policy permit-ping-iperf match destination-address
any
set security policies from-zone trust to-zone untrust policy permit-ping-iperf match application junos-
ping
set security policies from-zone trust to-zone untrust policy permit-ping-iperf match application iperf
set security policies from-zone trust to-zone untrust policy permit-ping-iperf then permit
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set applications application iperf protocol tcp
set applications application iperf destination-port 5001

root@csrx>
```

cSRX license:

```
root@csrx> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  anti_spam_key_sbl                     0            1           0    2025-10-14 00:00:00 UTC
  idp-sig                               0            1           0    2025-10-14 00:00:00 UTC
  appid-sig                             0            1           0    2025-10-14 00:00:00 UTC
  av_key_sophos_engine                  0            1           0    2025-10-14 00:00:00 UTC
  wf_key_websense_ewf                   0            1           0    2025-10-14 00:00:00 UTC
  cSRX                                  1            1           0    2025-10-14 00:00:00 UTC

Licenses installed:
  License identifier: f410a3dc-f128-4aad-8868-e62e8ddbf341
  License SKU: (NCKT)S-CSRX-A2_DEMOLAB
  License version: 1
  Order Type: demo
  Software Serial Number: 307102022020-rGYuC
  Customer ID: Juniper Internal
  License count: 1
  Features:
    anti_spam_key_sbl - Anti-Spam
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-14 00:00:00 UTC
    cSRX              - Containerized Firewall
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-14 00:00:00 UTC
    idp-sig           - IDP Signature
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-14 00:00:00 UTC
    appid-sig         - APPID Signature
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-14 00:00:00 UTC
    wf_key_websense_ewf - Web Filtering EWF
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-14 00:00:00 UTC
    av_key_sophos_engine - Anti Virus with Sophos Engine
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-14 00:00:00 UTC

root@csrx>
```

CSRX 24.2R1.17

cSRX version:

```
root@csrx> show version
Hostname: csrx
Model: csrx
Junos: 24.2R1.17
```

cSRX Configuration :

```
root@csrx> show configuration | display set
set version 20211201.145818_builder.r1226460
set interfaces ge-0/0/0 unit 0 family inet address 192.168.31.1/24
set interfaces ge-0/0/1 unit 0 family inet address 192.168.33.1/24
set security policies from-zone trust to-zone untrust policy permit-ping-iperf match source-address any
set security policies from-zone trust to-zone untrust policy permit-ping-iperf match destination-address
any
set security policies from-zone trust to-zone untrust policy permit-ping-iperf match application junos-
ping
set security policies from-zone trust to-zone untrust policy permit-ping-iperf match application iperf
set security policies from-zone trust to-zone untrust policy permit-ping-iperf then permit
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set applications application iperf protocol tcp
set applications application iperf destination-port 5001

root@csrx>
```

cSRX license:

```
root@csrx> show system license
License usage:
                                Licensed     Licensed    Licensed
                                 Feature      Feature     Feature
  Feature name                      used    installed      needed    Expiry
  Anti-Spam                            0            1           0    2025-10-15 00:00:00 UTC
  IDP-SIG                              0            1           0    2025-10-15 00:00:00 UTC
  APPID Signature                      0            1           0    2025-10-15 00:00:00 UTC
  Sophos AV                            0            1           0    2025-10-15 00:00:00 UTC
  Web Filtering EWF                    0            1           0    2025-10-15 00:00:00 UTC
  cSRX                                 1            1           0    2025-10-15 00:00:00 UTC

Licenses installed:

  License identifier: DemoLabJUNOS520607852
  License version: 4
  Order Type: demo
  Software Serial Number: 307102022020-iW4br
  Customer ID: Juniper Internal
  Features:
    Anti-Spam        - Anti-Spam
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-15 00:00:00 UTC
    cSRX             - Containerized SRX Firewall
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-15 00:00:00 UTC
    Sophos AV        - Anti Virus with Sophos Engine
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-15 00:00:00 UTC
    Web Filtering EWF - Web Filtering EWF
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-15 00:00:00 UTC
```

```
    APPID Signature  - APPID Signature
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-15 00:00:00 UTC
    IDP-SIG          - IDP Signature
      date-based, 2024-10-14 00:00:00 UTC - 2025-10-15 00:00:00 UTC

  License identifier: E20210503001
  License version: 4
  Order Type: trial
  Software Serial Number: 050320210001
  Customer ID: CSRX-JUNIPEREVAL
  Features:
    cSRX             - Containerized SRX Firewall
      date-based, 2024-11-27 14:46:37 UTC - 2025-01-26 14:46:37 UTC

root@csrx>
```

```
azureuser@rke2:~/validation/csrx-rke2> kubectl get pods -n csrx -o wide

NAME                READY   STATUS    RESTARTS   AGE     IP           NODE   NOMINATED NODE   READINESS
GATES

csrx                1/1     Running   0          5d18h   10.42.0.44   rke2   <none>           <none>

ubuntuapp-private   1/1     Running   0          6d23h   10.42.0.30   rke2   <none>           <none>

ubuntuapp-public    1/1     Running   0          6d23h   10.42.0.32   rke2   <none>           <none>

azureuser@rke2:~/validation/csrx-rke2> kubectl describe pods -n csrx

Name:             csrx

Namespace:        csrx

Priority:         0

Service Account:  default

Node:             rke2/10.0.0.4

Start Time:       Wed, 27 Nov 2024 14:46:30 +0000

Labels:           <none>

Annotations:      cni.projectcalico.org/containerID:
1f81c0315e6dd4c6ae92b3e81bb24ddb6856dd1e8290cb4198ca4176a462f1e9

                  cni.projectcalico.org/podIP: 10.42.0.44/32

                  cni.projectcalico.org/podIPs: 10.42.0.44/32

                  k8s.v1.cni.cncf.io/network-status:

                    [{

                        "name": "csrx/network-conf-1",

                        "interface": "eth1",

                        "mac": "fa:39:9a:a4:41:26",

                        "dns": {}

                    },{

                        "name": "csrx/network-conf-2",
```

```
                        "interface": "eth2",
                        "mac": "92:bf:69:30:12:ed",
                        "dns": {}
                    }]
                  k8s.v1.cni.cncf.io/networks: network-conf-1@eth1, network-conf-2@eth2
Status:           Running
IP:               10.42.0.44
IPs:
  IP:  10.42.0.44
Containers:
  csrx:
    Container ID:   containerd://c9c7e0d853318d38eb10b49ea82ad42e689433b3d80af61436f00b9c260872d5
    Image:          quay.io/juniper-128t/csrx:24.2R1.17
    Image ID:       quay.io/juniper-
128t/csrx@sha256:ef23e8b4d9b669bd635ea0fc2e56d32a0e238336722e3efb6b7f03aca26640af
    Port:           <none>
    Host Port:      <none>
    State:          Running
      Started:      Wed, 27 Nov 2024 14:46:32 +0000
    Ready:          True
    Restart Count:  0
    Limits:
      cpu:     4
      memory:  6000Mi
    Requests:
      cpu:     2
      memory:  4000Mi
    Environment:
      CSRX_ROOT_PASSWORD:  lab123
      CSRX_SIZE:           large
      CSRX_HUGEPAGES:      no
      CSRX_PACKET_DRIVER:  interrupt
      CSRX_FORWARD_MODE:   routing
      CSRX_LICENSE_FILE:   /var/jail/.csrx_license
      CSRX_JUNOS_CONFIG:   var/jail/csrx_config
```

```
      CSRX_LICENSE_FILE:   yes
      CSRX_CONFIG_FILE:    yes
      CSRX_PORT_NUM:       3
    Mounts:
      /var/jail from config (rw)
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-n7lrg (ro)
Conditions:
  Type                        Status
  PodReadyToStartContainers   True
  Initialized                 True
  Ready                       True
  ContainersReady             True
  PodScheduled                True
Volumes:
  config:
    Type:      ConfigMap (a volume populated by a ConfigMap)
    Name:      csrx-config-map
    Optional:  false
  kube-api-access-n7lrg:
    Type:                     Projected (a volume that contains injected data from multiple sources)
    TokenExpirationSeconds:   3607
    ConfigMapName:            kube-root-ca.crt
    ConfigMapOptional:        <nil>
    DownwardAPI:              true
QoS Class:                    Burstable
Node-Selectors:               <none>
Tolerations:                  node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                              node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events:                       <none>



Name:             ubuntuapp-private
Namespace:        csrx
Priority:         0
```

```
Service Account:  default
Node:             rke2/10.0.0.4
Start Time:       Tue, 26 Nov 2024 10:29:12 +0000
Labels:           app=ubuntuapp
                  zone=private
Annotations:      cni.projectcalico.org/containerID:
d1c772dcb1590e2ca522afd6be2fc12d35332e9f9522c9a396a859e3426a3795
                  cni.projectcalico.org/podIP: 10.42.0.30/32
                  cni.projectcalico.org/podIPs: 10.42.0.30/32
                  k8s.v1.cni.cncf.io/network-status:
                    [{
                        "name": "csrx/network-conf-1",
                        "interface": "net1",
                        "mac": "d6:bb:2d:eb:75:ae",
                        "dns": {}
                    }]
                  k8s.v1.cni.cncf.io/networks: [{ "name": "network-conf-1" }]
                  k8s.v1.cni.cncf.io/networks-status:
                    [{
                        "name": "network-conf-1",
                        "interface": "net1",
                        "ips": [
                            "192.168.31.11"
                        ],
                        "mac": "22:2f:60:a5:ff:01",
                        "dns": {}
                    }]
Status:           Running
IP:               10.42.0.30
IPs:
  IP:  10.42.0.30
Containers:
  ubuntuapp:
    Container ID:  containerd://987640ddb26e9155251b210844babe9de7344e000a2782a1c370d4f6c3b59386
    Image:         ubuntu-upstart
```

```
    Image ID:      sha256:caf860ff39ff6acbecc1e01d86d0a22e6a59b5fb10dc624e2c638161fc7dfa37
    Port:          <none>
    Host Port:     <none>
    Command:
      sh
      -c
      ifconfig net1 192.168.31.11/24;route add -net 192.168.33.0/24 gw 192.168.31.1;mount
/sys/fs/selinux -o remount,ro; apt install iperf; apt install ethtool; ethtool -K net1 tx off; sleep 40;
iperf -c 192.168.33.11 -t 300;sleep 100d
    State:          Running
      Started:      Tue, 26 Nov 2024 10:29:14 +0000
    Ready:          True
    Restart Count:  0
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-dmgxv (ro)
Conditions:
  Type                        Status
  PodReadyToStartContainers   True
  Initialized                 True
  Ready                       True
  ContainersReady             True
  PodScheduled                True
Volumes:
  kube-api-access-dmgxv:
    Type:                    Projected (a volume that contains injected data from multiple sources)
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
    DownwardAPI:             true
QoS Class:                   BestEffort
Node-Selectors:              <none>
Tolerations:                 node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events:                      <none>
```

```
Name:             ubuntuapp-public
Namespace:        csrx
Priority:         0
Service Account:  default
Node:             rke2/10.0.0.4
Start Time:       Tue, 26 Nov 2024 10:30:02 +0000
Labels:           app=ubuntuapp
                  zone=public
Annotations:      cni.projectcalico.org/containerID:
bf86b900ed80848e2f562c3d9aab77667df5764f9d3818ae535f281a3a26dc47
                  cni.projectcalico.org/podIP: 10.42.0.32/32
                  cni.projectcalico.org/podIPs: 10.42.0.32/32
                  k8s.v1.cni.cncf.io/network-status:
                    [{
                        "name": "csrx/network-conf-2",
                        "interface": "net1",
                        "mac": "ae:01:32:4d:a8:e9",
                        "dns": {}
                    }]
                  k8s.v1.cni.cncf.io/networks: [{ "name": "network-conf-2" }]
                  k8s.v1.cni.cncf.io/networks-status:
                    [{
                        "name": "network-conf-2",
                        "interface": "net1",
                        "ips": [
                            "192.168.33.11"
                        ],
                        "mac": "22:2f:60:a5:ff:02",
                        "dns": {}
                    }]
Status:           Running
IP:               10.42.0.32
IPs:
```

```
  IP:  10.42.0.32
Containers:
  ubuntuapp:
    Container ID:  containerd://849f4f7dd00d64a01af69c99bf9f4bd951c63ec8168e87e9f0991c45188bc2c4
    Image:         ubuntu-upstart
    Image ID:      sha256:caf860ff39ff6acbecc1e01d86d0a22e6a59b5fb10dc624e2c638161fc7dfa37
    Port:          <none>
    Host Port:     <none>
    Command:
      sh
      -c
      ifconfig net1 192.168.33.11/24;route add -net 192.168.31.0/24 gw 192.168.33.1;mount
/sys/fs/selinux -o remount,ro; apt install iperf; apt install ethtool; ethtool -K net1 tx off;iperf -s
    State:          Running
      Started:      Tue, 26 Nov 2024 10:30:04 +0000
    Ready:          True
    Restart Count:  0
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-tqztd (ro)
Conditions:
  Type                        Status
  PodReadyToStartContainers   True
  Initialized                 True
  Ready                       True
  ContainersReady             True
  PodScheduled                True
Volumes:
  kube-api-access-tqztd:
    Type:                    Projected (a volume that contains injected data from multiple sources)
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
    DownwardAPI:             true
QoS Class:                   BestEffort
```

```
Node-Selectors:              <none>
Tolerations:                 node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events:                      <none>
```

```
azureuser@rke2:~/validation/csrx-rke2> kubectl get network-attachment-definition -n csrx
NAME             AGE
network-conf-1   6d23h
network-conf-2   6d23h
```

```
azureuser@rke2:~/validation/csrx-rke2> kubectl describe network-attachment-definition -n csrx
Name:         network-conf-1
Namespace:    csrx
Labels:       <none>
Annotations:  <none>
API Version:  k8s.cni.cncf.io/v1
Kind:         NetworkAttachmentDefinition
Metadata:
  Creation Timestamp:  2024-11-26T10:29:03Z
  Generation:          1
  Resource Version:    828372
  UID:                 b02923d2-9158-4ac2-aac1-a09a4197388d
Spec:
  Config:  { "cniVersion": "0.3.0", "type": "bridge", "master": "eno2", "promiscMode": true }
Events:    <none>



Name:         network-conf-2
Namespace:    csrx
Labels:       <none>
Annotations:  <none>
API Version:  k8s.cni.cncf.io/v1
Kind:         NetworkAttachmentDefinition
Metadata:
```

```
  Creation Timestamp:  2024-11-26T10:29:03Z
  Generation:          1
  Resource Version:    828373
  UID:                 c82dd883-e61e-4487-971a-9d9fbc3b0dbd
Spec:
  Config:  { "cniVersion": "0.3.0", "type": "bridge", "master": "eno3", "promiscMode": true }
Events:    <none>
azureuser@rke2:~/validation/csrx-rke2>
```

Validation tests

IPERF TRAFFIC IS ALLOWED FROM ZONE TRUST (PRIVATE) TO ZONE UNTRUST (PUBLIC)

cSRX 21.1R3.11

```
root@csrx> show security flow session extensive
Session ID: 222, Status: Normal, State: Stand-alone
Flags: 0x40/0x0/0x2/0x8003
Policy name: permit-ping-iperf/4
Source NAT pool: Null
Dynamic application: junos:UNKNOWN,
Encryption:  Unknown
Url-category:  Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 1800, Current timeout: 1800
Session State: Valid
Start time: 2348, Duration: 14
   In: 192.168.31.11/53866 --> 192.168.33.11/5001;tcp,
  Conn Tag: 0x0, Interface: ge-0/0/0.0,
    Session token: 0xa, Flag: 0x1021
    Route: 0x90010, Gateway: 192.168.31.11, Tunnel ID: 0, Tunnel type: None
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 523562, Bytes: 785338688
   Out: 192.168.33.11/5001 --> 192.168.31.11/53866;tcp,
  Conn Tag: 0x0, Interface: ge-0/0/1.0,
    Session token: 0x14, Flag: 0x1020
    Route: 0xa0010, Gateway: 192.168.33.11, Tunnel ID: 0, Tunnel type: None
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 260258, Bytes: 13546792
Total sessions: 1

root@csrx> show security flow session
Session ID: 222, Policy name: permit-ping-iperf/4, State: Stand-alone, Timeout: 1800, Valid
  In: 192.168.31.11/53866 --> 192.168.33.11/5001;tcp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 5182650,
Bytes: 7773970688,
  Out: 192.168.33.11/5001 --> 192.168.31.11/53866;tcp, Conn Tag: 0x0, If: ge-0/0/1.0, Pkts: 2572593,
Bytes: 133842372,
Total sessions: 1

root@csrx>
```

```
root@ubuntuapp-private:/# iperf -c 192.168.33.11 -t 300
------------------------------------------------------------
Client connecting to 192.168.33.11, TCP port 5001
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.31.11 port 53866 connected with 192.168.33.11 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-300.0 sec  15.0 GBytes   429 Mbits/sec
root@ubuntuapp-private:/#
```

cSRX 24.2R1.17

```
root@csrx> show security flow session extensive
Session ID: 50, Status: Normal
Flags: 0x40/0x0/0x2/0x8003
Policy name: default-policy-logical-system-00/2
Source NAT pool: Null
Dynamic application: junos:UNKNOWN,
Encryption:  Unknown
Url-category:  Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 1800, Current timeout: 1800
Session State: Valid
Start time: 1733219595, Duration: 15
   In: 192.168.31.11/35074 --> 192.168.33.11/5001;tcp,
  Conn Tag: 0x0, Attachment Id: 0, GW Endpoint Id: 0, Flow Cookie: 0, Interface: ge-0/0/0.0,
    Session token: 0x8, Flag: 0x201021,
    Power-Mode Active: False
    Route: 0x50010, Gateway: 192.168.31.11, Tunnel ID: 0, Tunnel type: None,
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 481126, Bytes: 721684688
   Out: 192.168.33.11/5001 --> 192.168.31.11/35074;tcp,
  Conn Tag: 0x0, Interface: ge-0/0/1.0,
    Session token: 0x9, Flag: 0x201020,
    Power-Mode Active: False
    Route: 0x40010, Gateway: 192.168.33.11, Tunnel ID: 0, Tunnel type: None,
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 236025, Bytes: 12282092
Total sessions: 1

root@csrx> show security flow session
Session ID: 50, Policy name: default-policy-logical-system-00/2, Timeout: 1800, Session State: Valid
  In: 192.168.31.11/35074 --> 192.168.33.11/5001;tcp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 748618,
Bytes: 1122922688,
  Out: 192.168.33.11/5001 --> 192.168.31.11/35074;tcp, Conn Tag: 0x0, If: ge-0/0/1.0, Pkts: 367452,
Bytes: 19119608,
Total sessions: 1

root@csrx>
```

```
root@ubuntuapp-private:/# iperf -c 192.168.33.11 -t 300
------------------------------------------------------------
Client connecting to 192.168.33.11, TCP port 5001
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.31.11 port 35074 connected with 192.168.33.11 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-300.0 sec  14.1 GBytes   405 Mbits/sec
root@ubuntuapp-private:/#
```

TCP IPERF IS ALLOWED BUT UDP IPERF IS DENIED BY CSRX SECURITY POLICIES:

cSRX 21.1R3.11

```
root@ubuntuapp-private:/# iperf -c 192.168.33.11 -t 10
------------------------------------------------------------
Client connecting to 192.168.33.11, TCP port 5001
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.31.11 port 41642 connected with 192.168.33.11 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec   506 MBytes   423 Mbits/sec
root@ubuntuapp-private:/# iperf -c 192.168.33.11 -t 10 -u
------------------------------------------------------------
Client connecting to 192.168.33.11, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 192.168.31.11 port 46124 connected with 192.168.33.11 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 893 datagrams
[  3] WARNING: did not receive ack of last datagram after 10 tries.
root@ubuntuapp-private:/#
```

cSRX 24.2R1.17

```
root@ubuntuapp-private:/# iperf -c 192.168.33.11 -t 10
------------------------------------------------------------
Client connecting to 192.168.33.11, TCP port 5001
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.31.11 port 44922 connected with 192.168.33.11 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec   464 MBytes   389 Mbits/sec
root@ubuntuapp-private:/# iperf -c 192.168.33.11 -t 10 -u
------------------------------------------------------------
Client connecting to 192.168.33.11, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 192.168.31.11 port 51201 connected with 192.168.33.11 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  1.23 MBytes  1.03 Mbits/sec
[  3] Sent 893 datagrams
read failed: Connection refused
[  3] WARNING: did not receive ack of last datagram after 5 tries.
root@ubuntuapp-private:/#
```

ICMP PING TRAFFIC IS ALLOWED ONLY FROM TRUST ZONE TO UNTRUST ZONE

Same outputs with cSRX 21.1R3.11 and cSRX 24.2R1.17

```
root@ubuntuapp-private:/# ping 192.168.33.11
PING 192.168.33.11 (192.168.33.11) 56(84) bytes of data.
64 bytes from 192.168.33.11: icmp_seq=1 ttl=63 time=0.243 ms
64 bytes from 192.168.33.11: icmp_seq=2 ttl=63 time=0.173 ms
64 bytes from 192.168.33.11: icmp_seq=3 ttl=63 time=0.169 ms
64 bytes from 192.168.33.11: icmp_seq=4 ttl=63 time=0.195 ms
64 bytes from 192.168.33.11: icmp_seq=5 ttl=63 time=0.193 ms
64 bytes from 192.168.33.11: icmp_seq=6 ttl=63 time=0.173 ms
64 bytes from 192.168.33.11: icmp_seq=7 ttl=63 time=0.169 ms
64 bytes from 192.168.33.11: icmp_seq=8 ttl=63 time=0.172 ms
64 bytes from 192.168.33.11: icmp_seq=9 ttl=63 time=0.174 ms
^C
--- 192.168.33.11 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8181ms
rtt min/avg/max/mdev = 0.169/0.184/0.243/0.026 ms
root@ubuntuapp-private:/#
```

```
root@csrx> show security flow session
Session ID: 1130, Policy name: permit-ping-iperf/4, State: Stand-alone, Timeout: 2, Valid
  In: 192.168.31.11/155 --> 192.168.33.11/3;icmp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 1, Bytes: 84,
  Out: 192.168.33.11/3 --> 192.168.31.11/155;icmp, Conn Tag: 0x0, If: ge-0/0/1.0, Pkts: 1, Bytes: 84,

Session ID: 1131, Policy name: permit-ping-iperf/4, State: Stand-alone, Timeout: 2, Valid
  In: 192.168.31.11/155 --> 192.168.33.11/4;icmp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 1, Bytes: 84,
  Out: 192.168.33.11/4 --> 192.168.31.11/155;icmp, Conn Tag: 0x0, If: ge-0/0/1.0, Pkts: 1, Bytes: 84,

Session ID: 1132, Policy name: permit-ping-iperf/4, State: Stand-alone, Timeout: 4, Valid
  In: 192.168.31.11/155 --> 192.168.33.11/5;icmp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 1, Bytes: 84,
  Out: 192.168.33.11/5 --> 192.168.31.11/155;icmp, Conn Tag: 0x0, If: ge-0/0/1.0, Pkts: 1, Bytes: 84,

Session ID: 1133, Policy name: permit-ping-iperf/4, State: Stand-alone, Timeout: 4, Valid
  In: 192.168.31.11/155 --> 192.168.33.11/6;icmp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 1, Bytes: 84,
  Out: 192.168.33.11/6 --> 192.168.31.11/155;icmp, Conn Tag: 0x0, If: ge-0/0/1.0, Pkts: 1, Bytes: 84,
Total sessions: 4

root@csrx>
```

```
root@ubuntuapp-public:/# ping 192.168.31.11
PING 192.168.31.11 (192.168.31.11) 56(84) bytes of data.
^C
--- 192.168.31.11 ping statistics ---
19 packets transmitted, 0 received, 100% packet loss, time 18423ms

root@ubuntuapp-public:/#
```

```
root@csrx> show security flow session
Total sessions: 0

root@csrx>
```

OTHER TRAFFIC THAN IPERF (TCP PORT 5001) AND ICMP PING ARE REJECTED:

Same outputs with cSRX 21.1R3.11 and cSRX 24.2R1.17

```
root@csrx> show security flow statistics
    Current sessions: 0
    Packets received: 18193307
    Packets transmitted: 18192373
    Packets forwarded/queued: 0
    Packets copied: 0
    Packets dropped: 934
    Services-offload packets processed: 0
    Fragment packets: 0
    Pre fragments generated: 0
    Post fragments generated: 0

root@csrx>
```

```
root@ubuntuapp-private:/# ssh 192.168.33.11
…
…
```

```
root@ubuntuapp-public:/# tcpdump -i net1 port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on net1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@ubuntuapp-public:/#
```

```
root@csrx> show security flow statistics
    Current sessions: 0
    Packets received: 18193317
    Packets transmitted: 18192373
    Packets forwarded/queued: 0
    Packets copied: 0
    Packets dropped: 944
    Services-offload packets processed: 0
    Fragment packets: 0
    Pre fragments generated: 0
    Post fragments generated: 0

root@csrx>
```

Juniper Networks, Inc. Disclaimer

Juniper Networks Inc. (“Juniper”) is extremely pleased to present this proposal for your evaluation and consideration. Please note that the information contained in this proposal is proprietary and confidential to Juniper and is furnished in confidence to you with the understanding that it will not, without the express written permission of Juniper, be used or disclosed for other than proposal evaluation purposes.

For public sector customers, please note that this proposal may include information of a type that Juniper considers to be a trade secret and not subject to disclosure under any public records act. In the event such information is provided to you, Juniper retains all rights and remedies available under the public records act and requests that you provide us with written notice and an opportunity to respond in the event that a third party seeks disclosure of all or part of this response pursuant to such statutes. Juniper recognizes that public sector customers have particular procurement rules and processes that they must follow, and we will gladly work with you to ensure that we appropriately address and follow your procurement rules and processes.

This proposal is not, and should not be construed as, an offer to contract with Juniper. If you ultimately decide to purchase any or all of the products and/or services described in this proposal directly with Juniper, then all terms and conditions (inclusive of all business terms and conditions) will only be pursuant to a final and definitive written agreement, in the form of either: (i) an existing written agreement between us, or (ii) a mutually negotiated final written agreement. For purposes of clarity, for a direct relationship with Juniper, the final agreement would replace any other suggested terms and conditions, and Juniper hereby takes exceptions to any such purported terms and conditions. Notwithstanding anything to the contrary, Juniper makes no representations, warranties, or covenants in this proposal (including without limitation as to any products, services, service levels, third-party products or services or interoperability) separate from, in contravention of, or in addition to those contained in the final agreement, and any purported representation, warranty or covenant in this proposal shall be of no force or effect. If you desire a direct relationship with Juniper, we will welcome the opportunity to discuss mutually acceptable terms and conditions.

Alternatively, you may choose, and Juniper may require you, to purchase the Juniper products and services through a Juniper authorized reseller, and the terms and conditions, and all pricing, would be governed by your contract with a such reseller. Juniper cannot, in any fashion, dictate or control resale pricing.

Any information contained in this proposal relating to pricing or to future technology under development may be subject to change, including as a result of the negotiations which might occur in contemplation of the final agreement. If any pricing is provided by Juniper in this proposal, it is provided solely for your convenience and budgetary purposes only and does not constitute a bid or an offer from Juniper. Any other pricing will be provided directly by an authorized reseller, and any discussions relating thereto should be held directly with such reseller and not Juniper. Any descriptions, documentation, or references to third-party products not on Juniper’s price list are provided for informational purposes only and shall not be considered a part of Juniper’s proposal.

Thank you for considering Juniper for this exciting opportunity. We look forward to further assisting you with your technology requirements.