

Firewall Policy Use Case Reference



Modified: 2017-12-12

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Firewall Policy Use Case Reference

Copyright © 2017 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Chapter 1	Configuring Firewall Policies	5
	Firewall Policy Overview	5
	Firewall Policy Use Case Overview	6
	Firewall Policy Use Cases	6
	Firewall Policy Use Case - 1	7
	Firewall Policy Use Case - 2	9
	Firewall Policy Use Case - 3	11
	Firewall Policy Use Case - 4	12
	Firewall Policy Use Case - 5	13
	Firewall Policy Use Case - 6	13
	Firewall Policy Use Case - 7	14
	Firewall Policy Use Case - 8	14

CHAPTER 1

Configuring Firewall Policies

- [Firewall Policy Overview on page 5](#)
- [Firewall Policy Use Case Overview on page 6](#)
- [Firewall Policy Use Cases on page 6](#)

Firewall Policy Overview

Contrail Service Orchestration (CSO) provides the ability to create, modify, and delete firewall policy intents associated with a firewall policy. Firewall policies are presented as *intent-based policies*. A firewall policy intent controls transit traffic within a context that is derived out of the end-points defined in the intent. Intent-based firewall policies can incorporate both transport layer (Layer 4) and application layer (Layer 7) firewall constructs in a single intent. The underlying system, automatically analyzes the intent, translates them into the set of rules the devices understand. The choice of sequence and the assignment happens implicitly based on the endpoints in the intent definition. The intent consist of source and destination endpoints. Endpoints could be applications (L7), sites or site groups, IP address/address-groups, services, or departments.

For more information on the procedures for creating firewall policies and firewall policy intents, see *About the Firewall Policy Page*.



NOTE: Intent based policies are not applicable for Hybrid WAN deployments.

Firewall policies provide security functionality by enforcing intents on traffic that passes through a device. Traffic is permitted or denied based on the action defined as the firewall policy intent.

A firewall policy provides the following features:

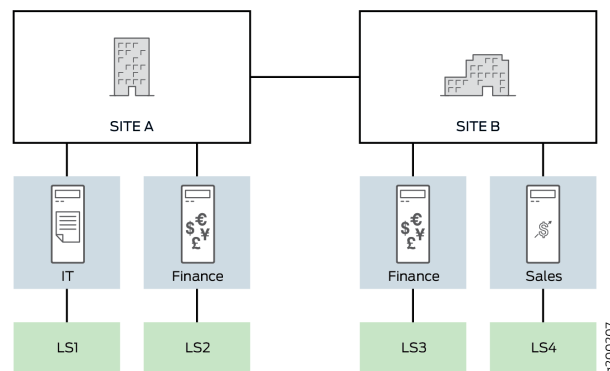
- Permits, rejects, or denies traffic based on the application in use.
- Identifies not only HTTP but also any application running on top of it, enabling you to properly enforce policies. For example, an application firewall intent could block HTTP traffic from Facebook but allow Web access to HTTP traffic from Microsoft Outlook.
- Provides the ability to perform threat management on permitted traffic using UTM profiles. For more information on UTM profiles, see *UTM Overview*.

Firewall Policy Use Case Overview

The following use cases provide an understanding of how you can construct intent-based firewall policies for different traffic scenarios across sources and destinations, using various use cases.

The following topology is used for all the use cases:

Figure 1: Topology Diagram



The following are some definitions that are applicable to all the use cases:

- When you configure a site, you can specify the local breakout. Depending on the breakout you specifies, the zone is classified as trust or untrust. Traffic originating from within the network is classified as trust based traffic. Traffic originating from outside the network is classified as untrust.
- A trust zone refers to the overlay interface that contains all the GRE tunnel interfaces such as gr-0/0/0.1, gr-0/0/0.2, and IPSec interfaces such as SD 0.1, SD 0.2.
- An untrust zone refers to the underlay interfaces (underlying physical interfaces) such as GE000, GE001.
- Unless you select a specific address or service as a destination endpoint, Cloud CPE Solution considers it as **Any** service or address hosted on the Internet, unless qualified with a site.

Firewall Policy Use Cases

- [Firewall Policy Use Case - 1 on page 7](#)
- [Firewall Policy Use Case - 2 on page 9](#)
- [Firewall Policy Use Case - 3 on page 11](#)
- [Firewall Policy Use Case - 4 on page 12](#)
- [Firewall Policy Use Case - 5 on page 13](#)
- [Firewall Policy Use Case - 6 on page 13](#)

- [Firewall Policy Use Case - 7 on page 14](#)
- [Firewall Policy Use Case - 8 on page 14](#)

Firewall Policy Use Case - 1

Define a firewall policy that permits traffic to and from the departments in site A and the departments in site B, where:

- Site A has two departments - Engineering (LAN segment LS1 and LS2) and Finance (LAN segment LS3 and LS4).
- Site B has two departments - IT (LAN segment LS5 and LS6) and Admin (LAN segment LS7 and LS8).

[Table 1 on page 7](#) shows the firewall policy intent that is defined:

Table 1: Firewall Policy Definition for Use Case - 1

Source	Destination (Application)	Action
site A	site B	Permit

[Table 2 on page 7](#) shows how this firewall policy intent is resolved:

Table 2: Firewall Policy Intent Resolution for Use Case - 1

Site	Source Department	Source Address	Zone	Destination Address	Service	Intent Created
site A	Engineering	[LS1, LS2]	Trust	[LS5, LS6, LS7, LS8]	Any	Intent 1__0
	Finance	[LS3, LS4]	Trust	[LS5, LS6, LS7, LS8]	Any	Intent 1__1
site B	Trust	[LS5, LS6, LS7, LS8]	IT	[LS5, LS6]	Any	Intent 1__0
	Trust	[LS5, LS6, LS7, LS8]	Admin	[LS7, LS8]	Any	Intent 1__1

Configuration Example Configuration sample for Site A

```

Default policy: deny-all
From zone: trust, To zone: untrust
  Policy: allow_all, State: enabled, Index: 6, Scope Policy: 0, Sequence
number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: trust, To zone: trust
  Policy: allow_all, State: enabled, Index: 8, Scope Policy: 0, Sequence
number: 1
    Source addresses: any

```

```
    Destination addresses: any
    Applications: any
    Action: permit
From zone: oam, To zone: untrust
  Policy: allow_all, State: enabled, Index: 7, Scope Policy: 0, Sequence
number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: Sales, To zone: trust
  Policy: Intent_1__0, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1
    Source addresses: ls-183.1.1.0/24-s1-L2
    Destination addresses: ls-189.1.1.0/24-s2-L2, ls-184.1.1.0/24-s2-L1
    Applications: any
    Action: permit, application services
  Application traffic control: pr_cos_Sales
From zone: Finance, To zone: trust
  Policy: Intent_1__1, State: enabled, Index: 5, Scope Policy: 0, Sequence
number: 1
    Source addresses: ls-183.1.1.0/24-s1-L1
    Destination addresses: ls-189.1.1.0/24-s2-L2, ls-184.1.1.0/24-s2-L1
    Applications: any
    Action: permit, application services
```

Configuration sample for Site B

```
Default policy: deny-all
From zone: trust, To zone: untrust
  Policy: allow_all, State: enabled, Index: 6, Scope Policy: 0, Sequence
number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: trust, To zone: trust
  Policy: allow_all, State: enabled, Index: 8, Scope Policy: 0, Sequence
number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: trust, To zone: IT
  Policy: Intent_1__0, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1
    Source addresses: ls-183.1.1.0/24-s1-L2, ls-183.1.1.0/24-s1-L1
    Destination addresses: ls-189.1.1.0/24-s2-L2
    Applications: any
    Action: permit
From zone: trust, To zone: Finance
  Policy: Intent_1__1, State: enabled, Index: 5, Scope Policy: 0, Sequence
number: 1
    Source addresses: ls-183.1.1.0/24-s1-L2, ls-183.1.1.0/24-s1-L1
    Destination addresses: ls-184.1.1.0/24-s2-L1
    Applications: any
    Action: permit
From zone: oam, To zone: untrust
  Policy: allow_all, State: enabled, Index: 7, Scope Policy: 0, Sequence
number: 1
    Source addresses: any
```


Destination addresses: any
 Applications: any
 Action: permit

Firewall Policy Use Case - 2

Define a firewall policy that permits access to all departments in site A and site B to the internet, where:

- Site A has two departments - Engineering (LAN segment LS1 and LS2) and Finance (LAN segment LS3 and LS4).
- Site B has two departments - IT (LAN segment LS5 and LS6) and Admin (LAN segment LS7 and LS8).

Table 3 on page 9 shows the firewall policy intent that is defined:

Table 3: Firewall Policy Definition for Use Case - 2

Source	Destination (Application)	Action
site A	Internet	Permit
site B	Internet	Permit

Table 4 on page 9 shows how this firewall policy intent is resolved:

Table 4: Firewall Policy Intent Resolution for Use Case - 2

Site	Source Department	Source Address	Zone	Destination Address	Service	Intent Created
site A	Engineering	Any	Trust/Untrust	Any	http, https, icmp-ping, dns	Intent 1__0
	Finance	Any	Trust/Untrust	Any	http, https, icmp-ping, dns	Intent 1__1
site B	Engineering	Any	Trust/Untrust	Any	http, https, icmp-ping, dns	Intent 1__0
	Finance	Any	Trust/Untrust	Any	http, https, icmp-ping, dns	Intent 1__1

Configuration Example Configuration sample for site A to Internet

```

Default policy: deny-all
From zone: trust, To zone: untrust
Policy: allow_all, State: enabled, Index: 6, Scope Policy: 0, Sequence
number: 1
Source addresses: any
Destination addresses: any
Applications: any
Action: permit
From zone: trust, To zone: trust

```

```
Policy: allow_all, State: enabled, Index: 8, Scope Policy: 0, Sequence
number: 1
  Source addresses: any
  Destination addresses: any
  Applications: any
  Action: permit
From zone: oam, To zone: untrust
Policy: allow_all, State: enabled, Index: 7, Scope Policy: 0, Sequence
number: 1
  Source addresses: any
  Destination addresses: any
  Applications: any
  Action: permit
From zone: Sales, To zone: trust
Policy: Intent_1__0, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1
  Source addresses: ls-183.1.1.0/24-s1-L2
  Destination addresses: ls-189.1.1.0/24-s2-L2, ls-184.1.1.0/24-s2-L1
  Applications: any
  Action: permit, application services
  Application traffic control: pr_cos_Sales
From zone: Finance, To zone: trust
Policy: Intent_1__1, State: enabled, Index: 5, Scope Policy: 0, Sequence
number: 1
  Source addresses: ls-183.1.1.0/24-s1-L1
  Destination addresses: ls-189.1.1.0/24-s2-L2, ls-184.1.1.0/24-s2-L1
  Applications: any
  Action: permit, application services
```

Configuration sample for site B to Internet

```
root@A1DCAEBD0752.s2.Nithya> show security policies
Default policy: deny-all
From zone: trust, To zone: untrust
Policy: allow_all, State: enabled, Index: 6, Scope Policy: 0, Sequence
number: 1
  Source addresses: any
  Destination addresses: any
  Applications: any
  Action: permit
From zone: trust, To zone: trust
Policy: allow_all, State: enabled, Index: 8, Scope Policy: 0, Sequence
number: 1
  Source addresses: any
  Destination addresses: any
  Applications: any
  Action: permit
From zone: oam, To zone: untrust
Policy: allow_all, State: enabled, Index: 7, Scope Policy: 0, Sequence
number: 1
  Source addresses: any
  Destination addresses: any
  Applications: any
  Action: permit
From zone: IT, To zone: trust
Policy: Intent_1__0, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1
  Source addresses: any
  Destination addresses: any
  Applications: junos-https, junos-icmp-ping, junos-dns-udp, junos-http,
junos-dns-tcp
```

```

    Action: permit, application services
    Application traffic control: pr_cos_IT
    From zone: Finance, To zone: trust
    Policy: Intent_1__1, State: enabled, Index: 5, Scope Policy: 0, Sequence
    number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-https, junos-icmp-ping, junos-dns-udp, junos-http,
    junos-dns-tcp
    Action: permit, application services

```

Firewall Policy Use Case - 3

Define a firewall policy that permits access to all departments in site A and site B to Facebook, where:

- Site A has two departments - Engineering (LAN segment LS1 and LS2) and Finance (LAN segment LS3 and LS4).

Table 5 on page 11 shows the firewall policy intent that is defined:

Table 5: Firewall Policy Definition for Use Case - 3

Source	Destination (Application)	Action
site A	Facebook	Permit

Table 6 on page 11 shows how this firewall policy intent is resolved:

Table 6: Firewall Policy Intent Resolution for Use Case - 3

Site	Source Address	Zone	Destination Address	Service	Intent Created	Application Firewall Profile
site A	Any	Trust/Untrust	Facebook	Any	Intent 1__0	AppFwProfile_0

Configuration Example Configuration sample for site A to Facebook

```

root@100304238820.s1.Nithya> show security policies
Default policy: deny-all
From zone: trust, To zone: untrust
  Policy: allow_all, State: enabled, Index: 6, Scope Policy: 0, Sequence
  number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: trust, To zone: trust
  Policy: allow_all, State: enabled, Index: 8, Scope Policy: 0, Sequence
  number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: oam, To zone: untrust
  Policy: allow_all, State: enabled, Index: 7, Scope Policy: 0, Sequence

```

```

number: 1
  Source addresses: any
  Destination addresses: any
  Applications: any
  Action: permit
From zone: Sales, To zone: untrust
  Policy: Intent_1__0, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1
  Source addresses: ls-183.1.1.0/24-s1-L2
  Destination addresses: any
  Applications: any
  Action: permit, application services
  Application firewall: AppFwProfile_0
From zone: Finance, To zone: untrust
  Policy: Intent_1__1, State: enabled, Index: 5, Scope Policy: 0, Sequence
number: 1
  Source addresses: ls-183.1.1.0/24-s1-L1
  Destination addresses: any
  Applications: any
  Action: permit, application services
  Application firewall: AppFwProfile_0
root@100304238820.s1.Nithya> show configuration security application-firewall
rule-sets AppFwProfile_0 {
  rule rule-e0dbb5a9-0a98-496a-a898-f5794f9a717d-appFwRule {
    match {
      dynamic-application junos:FACEBOOK-APP;
      ssl-encryption any;
    }
    then {
      permit;
    }
  }
  default-rule {
    deny;
  }
}

```

Firewall Policy Use Case - 4

Define a firewall policy that controls access to specific applications for various departments, with the following intents:

- All PR departments located in site A and site B (which are in different geographical locations) are permitted to access the news applications BBC and CNN.
- All engineering departments located in site A and site B (which are in different geographical locations) are denied access to the news applications BBC and CNN.
- Access to Telnet and SSH applications is given only to the engineering department.
- Access to Telnet and SSH applications is denied to all departments, except for the engineering department.

Table 7 on page 13 shows the firewall policy intents that are to fulfil this requirement:

Table 7: Firewall Policy Use Case - 4

Source	Destination (Application)	Action
PR department, site A and PR department, site B	BBC and CNN	Permit
Engineering department, site A and Engineering department, site B	BBC and CNN	Deny
Engineering department	Telnet and SSH	Permit
Any (All addresses except the engineering department)	Telnet and SSH	Deny



NOTE: The number of intents depends on the number of source sites with the given department and the number of destination sites.

Firewall Policy Use Case - 5

Define a firewall policy that denies access to networking sites such as Facebook and Twitter (defined as application group Social Networking) to the HR, finance, and IT departments located in Site A.

Table 8 on page 13 shows the firewall policy intents that are needed to fulfil this requirement:

Table 8: Firewall Policy Use Case - 5

Source Department	Destination Application Group	Action
HR, Finance, IT, site A	Application group Social Networking (Facebook and Twitter)	Deny



NOTE: Add site A, only if the HR, Finance, or IT departments are present in different sites, but, you only want to apply this firewall policy intent to the HR, Finance, and IT departments present in site A, only.

Firewall Policy Use Case - 6

Define a firewall policy that controls traffic to example.com based on the services used by the source endpoint, with the following intents:

- The IT team in site A is permitted access to FTP and HTTP services.
- The IT team in site B is only permitted access to the FTP service.

Table 9 on page 14 shows the firewall policy intents that are needed to fulfil this requirement:

Table 9: Firewall Policy Use Case - 6

Source Address	Service	Destination Address	Action
IT, site A	FTP and HTTP	example.com	Permit
IT, site B	FTP	example.com	Permit

Firewall Policy Use Case - 7

Define a firewall policy that controls access to an address over the internet (HTTP) for various sites or site groups with the following intents:

- All addresses of site A and site B are permitted access to example.com.
- All addresses of site group Q1 are denied access to example-one.com.

Table 10 on page 14 shows the firewall policy intents that are needed to fulfil this requirement:

Table 10: Firewall Policy Use Case - 7

Source Address	Service	Destination Address	Action
IP address prefix, site A and IP-Prefix, site B	HTTP	www.example.com	Permit
IP address prefix, site group Q1	HTTP	www.example-one.com	Deny

Firewall Policy Use Case - 8

Define a firewall policy where a specific IP address belonging to all sites and departments, is permitted or denied the use HTTP or FTP as a service.

Table 11 on page 14 shows the firewall policy intents that are needed to fulfil this requirement:

Table 11: Firewall Policy Use Case - 8

Source Address	Service	Destination Address	Action
192.0.2.0	HTTP	example.com	Permit
192.0.2.0	FTP	example.com	Deny