JUNIPER NETWORKS SRX SERIES SERVICES GATEWAYS/ WEBSENSE V10000

SRX Series Configuration to Enable Security Solutions with TRITON

Although Juniper Networks has attempted to provide accurate information in this guide, Juniper Networks does not warrant or guarantee the accuracy of the information provided herein. Third party product descriptions and related technical details provided in this document are for information purposes only and such products are not supported by Juniper Networks. All information provided in this guide is provided "as is", with all faults, and without warranty of any kind, either expressed or implied or statutory. Juniper Networks and its suppliers hereby disclaim all warranties related to this guide and the information contained herein, whether expressed or implied of statutory including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement, or arising from a course of dealing, usage, or trade practice.

Copyright © 2010, Juniper Networks, Inc.

Table of Contents

Table of Figures

Copyright © 2010, Juniper Networks, Inc.

Introduction

A powerful new paradigm of Internet-enabled relationships is transforming businesses across the globe. Companies that embrace "Web 2.0" technologies empower effective and lasting connections with employees, customers, and partners. These are powerful tools that can create and sustain competitive advantage—but the underlying technologies can also expose the business to complex and dynamic new risks. Juniper Networks® SRX Series Services Gateways, combined with Websense's V10000 Web Security Gateways, help companies enjoy the benefits of Web 2.0 solutions while mitigating the associated security challenges with power, speed, and flexibility.

Scope

This document is targeted at system engineers, network administrators, and other technical audiences interested in designing and implementing Juniper Networks SRX Series Services Gateways with Websense TRITON V10000 Web Security Gateway appliances.

Design Considerations

Figure 1 illustrates a common network design solution using the SRX Series and V10000 appliances. The SRX Series is responsible for redirecting specific traffic from the User LAN --for example, HTTP/HTTPS --to the V10000 appliances. The network administrator configures the TRITON V10000 appliances to provide multi-vector inbound and outbound real-time content inspection to protect against malware and sensitive data loss. The policy-based user interface increases user productivity by basing privileges on user or group identity in your corporate user directory. The V10000 proxies user traffic to the Internet. When the user traffic is unauthorized based on protocol or dynamic website policy, the user's browser is redirected to the "Block Page" served by the V10000.

The enterprise network includes the SRX Series and the Websense TRITON V10000 appliances in the "management" segment of the network, and the enterprise users are identified in the "User LAN" segment of the network. This deployment architecture leverages the flexibility of the SRX Series to securely separate the user traffic from the network administration of the SRX Series and the Websense security appliances.

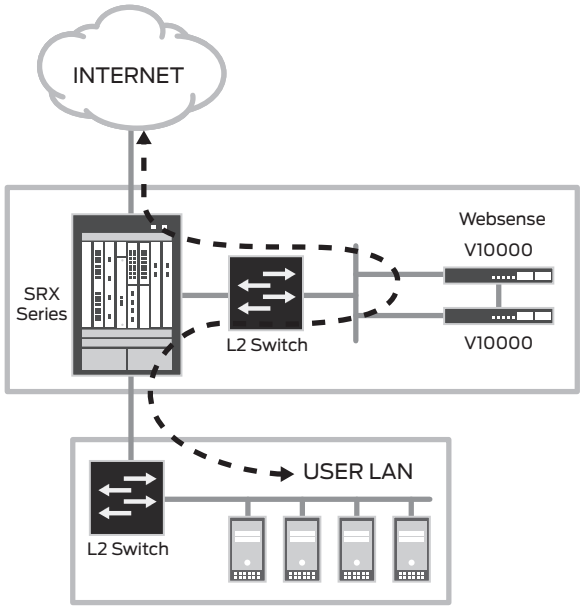

Figure 1: Reference network

For the one V10000 appliance solution, three physical ports are utilized: "C", "P1," and "N." The "C" port of the appliance is the management port through which the administrator manages the appliance. The "C" port is also the destination for the "Block Page" redirection. The "P1" port is the proxy port of the V10000 that provides the real-time malware and dynamic website classification. The SRX Series connects the V10000 to both the user LAN and the Internet. The "N" port is used to provide application and Web protocol-specific blocking and bandwidth throttling. Over 120 Web protocols are recognized by protocol "fingerprint" (this permits the identification of applications such as Skype, BitTorrent, and Yahoo Chat.) Malware "phone-home" communications are also recognized and denied access to the Internet. To implement this capability, a layer 2 switch is needed to mirror user traffic. When the P1 port allows user traffic, the V10000 establishes a new traffic flow (proxy) via the same P1 port. When traffic is not permitted, the V10000 issues a redirect message via the P1 port to the user browser. The user browser is redirected to a "Block Page" that is served by the V10000 at the C port. These two scenarios are illustrated in the following ladder diagrams.

Copyright © 2010, Juniper Networks, Inc.

Figure 2 illustrates the ladder diagram for user traffic allowed by the Websense V10000. The V10000 proxies the traffic between the user and the Internet via the V10000 P1 port. The proxied traffic is indicated by the separate dark gray and light gray traffic flows.

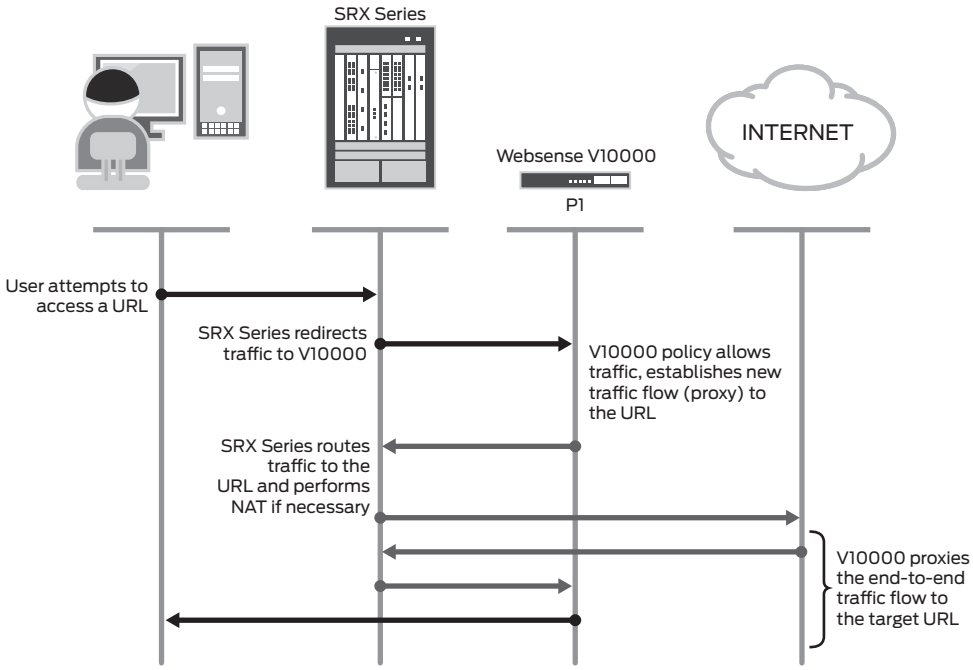

Figure 2: User traffic allowed

Figure 3 illustrates the ladder diagram for user traffic that is blocked and redirected by the V10000.

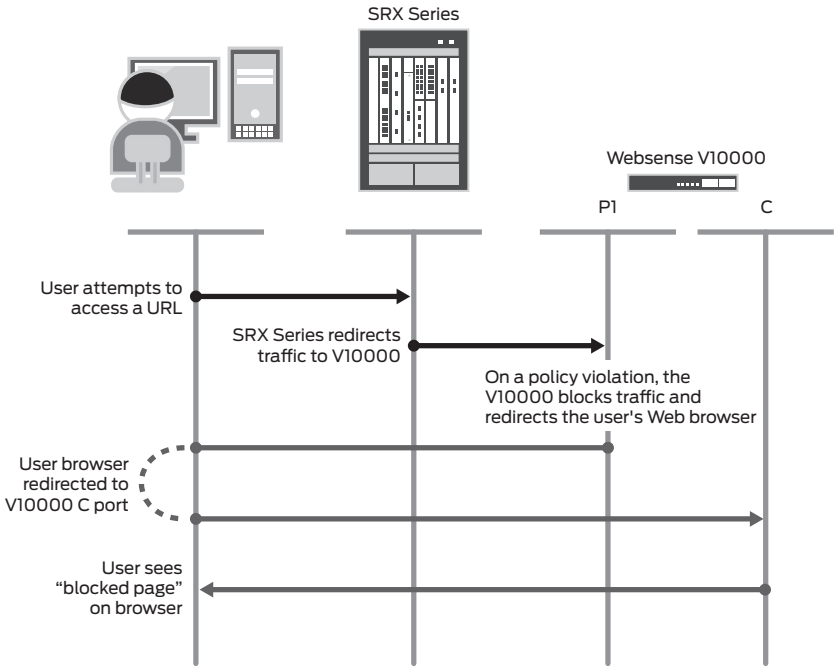

Figure 3: User traffic blocked

Copyright © 2010, Juniper Networks, Inc.

Protocol Operation

The Websense V10000 product uses TCP port 15871. This port service is used to insert an alert placed in-stream with the Web browser, thereby redirecting the Web browser to a "Block Page" served by the V10000 appliance. The Web browser is redirected to the V10000 "C" port. The "C" port is typically located in the management segment of the network, to which the User LAN would typically not have access. Therefore, the SRX Series security policy must be configured to permit the User LAN traffic to access the V10000 "C" port for TCP/15871.

The SRX Series uses the native Juniper Networks Junos® operating system filter-based forwarding (FBF) approach to redirect the traffic to the V10000. No special protocol is required to redirect traffic to the V10000.

Implementation

This section provides the step-by-step SRX Series configuration to support the joint solution. Figure 4 illustrates the reference network that is used throughput this implementation guide. The SRX Series administrator must set up four (4) separate security zones: *"public-inet"* (for access to the public Internet), *"user-lan"* (for access to the internal network), "management" (for access to the V10000's "C" port), and *"web-redirect"* (for access to V10000's P1 port). To keep the network diagram simple, each of the SRX Series physical interfaces are shown directly attached to the end devices. In a field deployment, these ports would most likely be connected via L2 switches.

The four security zones and the permitted traffic flows through the SRX Series are illustrated and explained in Table 1.

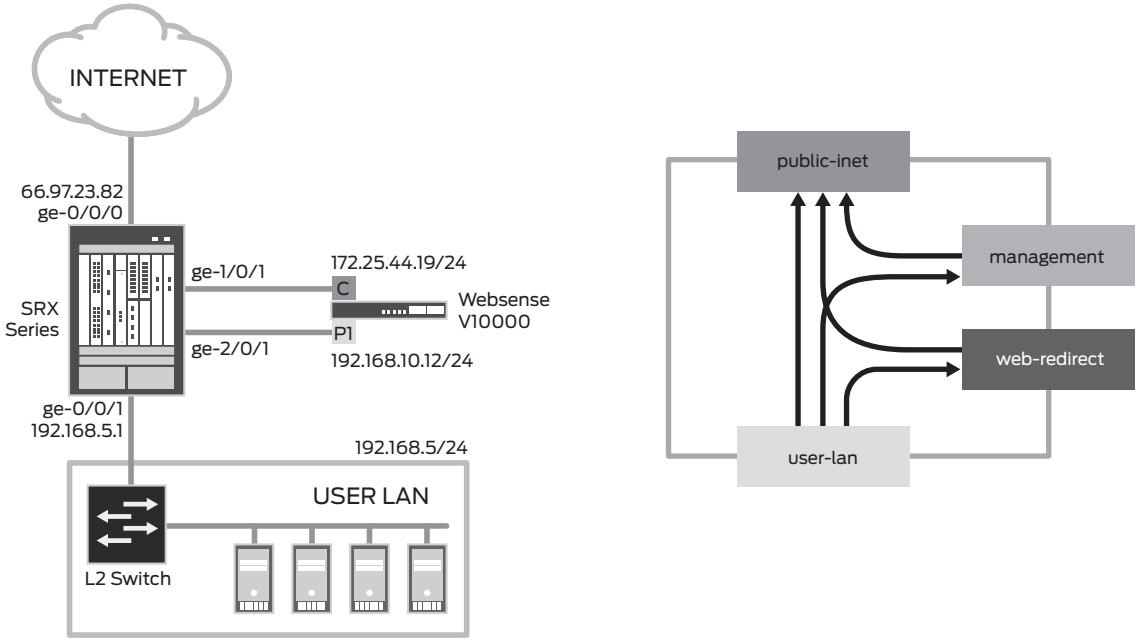

Figure 4: Example implementation network

Table 1: SRX Series Security Policies

FROM SECURITY ZONE	TO SECURITY ZONE	PURPOSE
user-lan	web-redirect	Redirected traffic to V10000 for security processing
web-redirect	public-inet	V10000 proxies allowed user traffic
user-lan	management	V10000 redirecting user browser to "Block Page"
user-lan	public-inet	User traffic that does not need to be processed by V10000
management	public-inet	V10000 control traffic that needs to access security databases for subscription updates and other functions

Copyright © 2010, Juniper Networks, Inc.

Implementation Tasks

The SRX Series administrator needs to perform the following configuration steps that are specific to creating an end-to-end solution with the Websense V10000 appliance.

1. Create the web-redirect security zone that provides access to the V10000 P1 port.
2. Create a FBF that is used to redirect specific traffic from the User LAN to the V10000 P1 port.
3. Add a security policy from user-lan to web-redirect. This step is necessary to allow any traffic to be redirected to the V10000. A separate access control filter list is used to explicitly specify which traffic is actually redirected.
4. Create an access control filter (called a "firewall filter" in Junos OS) to selectively identify the traffic to be redirected to the V10000. For the purpose of this implementation guide example, this is HTTP and HTTPS traffic only.
5. Attach the redirecting firewall-filter to the physical interface attached to the User LAN network segment.
6. Add a security policy from user-lan to public-inet. This step is necessary to allow traffic to the Internet that does not need to be processed by the Websense V10000.
7. Add the V10000 "C" port to the management security zone address book. This step is necessary so that the V10000 can redirect the user Web browser to the "C" port for blocked sites or Web protocols.
8. Create a Websense-specific security application definition for the Websense redirect protocol—TCP/15871.
9. Add a security policy from user-lan to management only to the V10000 "C" port and only for the TCP/15871 traffic. This step is necessary so that the user Web browser can be redirected to the V10000 "Block Page." Normally User LAN traffic should not be allowed to access the management security zone.
10. Add any Network Address Translation (NAT) necessary to support both web-redirect traffic as well as user-lan traffic out toward the public Internet.

There are two general approaches for configuring Junos OS devices for solution integration with partner products. The first, and most common, is manually provisioning these steps. This implementation guide presents this detailed information in a step-by-step fashion. The second approach, which is significantly easier to deploy, is using Junos OS self-provisioning for Websense. This implementation guide presents an example of such self-provisioning in the next section.

SRX Series Configuration Using Junos Automation

Junos OS natively supports the ability to extend and customize the configuration and operational elements of the SRX Series using Junos automation capabilities. The key benefit of using Junos automation is that the network administrator is not required to manually provision the SRX Series with the specific Junos OS commands. Instead, the administrator needs only to provision the relevant V10000 information, and the SRX Series automatically creates the required configuration. By using this technique, the administrator can be assured that all required configurations steps are properly completed, thereby reducing errors and enabling a faster installation.

For example, in the reference network the following is known:

- The management security zone is attached to SRX Series interface ge-1/0/1.
- The web-redirect security zone is attached to SRX Series interface ge-2/0/1.
- The V10000 appliance:
  - The C port inet address is 172.25.44.19
  - The P1 port inet address is 192.168.10.12
- The User LAN:
  - The SRX Series inet address is 192.168.5.1.
  - The User LAN network is 192.168.5.0 / 24.
  - The attached SRX Series interface is ge-0/0/1.
  - HTTP/HTTPS traffic should be redirected to V10000.

Copyright © 2010, Juniper Networks, Inc.

Junos OS could automatically configure all 10 steps described in the previous section using the following SRX Series configuration.

```
[edit]
admin@SRX# show groups
websense {
    apply-macro V10000-alpha {
        c-port 172.25.44.19;
        p1-port 192.168.10.12;
    }
    apply-macro user-lan {
        interface ge-0/0/1;
        address 192.168.5.1/24;
        redirect V10000-alpha;
    }
    apply-macro zones {
        management ge-1/0/1;
        web-redirect ge-2/0/1;
    }
}
```

This configuration shows an example use of Junos OS groups and apply-macros that can be used to organize the relevant information. This configuration concisely describes the solution details in one location under the “websense” group. A Junos OS commit script tailored for the Websense solution uses this information to automatically create the configuration outlined in the 10 steps.

SRX Series Configuration Step by Step

The alternate approach to using Junos automation is to create the configuration manually. This section presents the 10 steps outlined in the previous section.

1. Create the web-redirect security zone that provides access to the V10000 P1 port. This step is accomplished by defining a new security zone and identifying the interface toward the V10000 P1 port.

```
[edit]
admin@SRX# show security zones
security-zone web-redirect {
    interfaces {
        ge-2/0/1.0;
    }
}
```

Note that you should follow this step if the physical interface toward the V10000 P1 interface was already configured. If this is not the case, then use the following configuration at the interface hierarchy.

```
admin@SRX# show interfaces ge-2/0/1
description “To Websense V10000 P1 network”;
unit 0 {
    family inet {
        address 192.168.10.1/24;
    }
}
```

Copyright © 2010, Juniper Networks, Inc.

2. Create a FBF that is used to redirect specific traffic from the User LAN to the V10000 P1 port.

This technique requires a *forwarding-based routing-instance* that has a single next-hop route to the V10000 P1 port. The forwarding instance has an independent routing table, which is the basis for changing the routing rules for traffic processing. In order to populate the forwarder's routing table correctly, a *policy-statement* must be defined to only include routing for the interface going to the V10000 P1 port—in this case ge-2/0/1.

```
admin@SRX# show policy-options
policy-statement only-web-redirect-interface {
    term allow {
        from {
            instance master;
            interface ge-2/0/1.0;
        }
        then accept;
    }
    term reject {
        then reject;
    }
}
```

The next part is to define the forwarding instance and import only the interface route defined by the `only-web-redirect-interface` routing policy. The forwarding instance has a single next hop to the V10000 P1 address 192.168.10.12. This is the configuration that redirects all traffic to the V10000 P1 port for processing.

```
admin@SRK# show routing-instances
to-P1-V10000-alpha {
    instance-type forwarding;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 192.168.10.12;
        }
        instance-import only-web-redirect-interface;
    }
}
```

3. Add a security policy from user-lan to web-redirect. This step is necessary to *allow* any traffic to be redirected to the V10000. A separate access control list is used to explicitly specify which traffic is actually redirected.

```
admin@SRX# show security policies
from-zone user-lan to-zone web-redirect {
    policy permit-all {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

Note that you should follow this step if the user-lan security zone has already been set up. If it has not been set up, then do the following to first configure the physical interface and then the security zone. Within the security zone definition there is an address book definition that identifies the local hosts on the user-lan network. This address book definition is used in a later step involving a specific security policy.

Copyright © 2010, Juniper Networks, Inc.

```
admin@SRX# show interfaces ge-0/0/1
description “To User LAN network”;
unit 0 {
    family inet {
        address 192.168.5.1/24;
    }
}
admin@SRX# show security zones
security-zone user-lan {
    address-book {
        address local-hosts 192.168.5.0/24;
    }
    interfaces {
        ge-0/0/1.0;
    }
}
```

4. Create an access control filter (called a “firewall filter” in Junos OS) to selectively identify the traffic to be redirected to the V10000. For the purpose of this implementation guide example, this is HTTP and HTTPS traffic only. The following firewall configuration has two terms. The first term matches on the target redirect traffic (HTTP/HTTPS) and when found puts the traffic into the forwarding instance created in the prior step. That forwarding instance determines one thing—it forwards the traffic to the V10000 P1 port. The second term accepts all other (non-redirected) traffic. This term is very important, and if left out, all other traffic would be silently discarded. The reason for that is that a firewall filter has an implicit “deny” as a last term rule.

```
admin@SRX# show firewall
family inet {
    filter redirect-to-V10000-alpha {
        term web-traffic {
            from {
                protocol tcp;
                port [ http https ];
            }
            then {
                routing-instance to-P1-V10000-alpha;
            }
        }
        term default {
            then accept;
        }
    }
}
```

5. Attach the redirecting firewall-filter to the physical interface attached to the User LAN network segment. The filter created in the prior step is added to the physical interface as highlighted.

```
admin@SRX# show interfaces ge-0/0/1
description “To User LAN network”;
unit 0 {
    family inet {
        filter {
            input redirect-to-V10000-alpha;
        }
    }
}
```

Copyright © 2010, Juniper Networks, Inc.

6. Add a security policy from user-lan to public-inet. This step is necessary to allow traffic to the Internet that does not need to be processed by the Websense V10000.

```
admin@SRX# show security policies
from-zone user-lan to-zone public-inet {
    policy permit-all {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

Note that you should follow this step if the public-inet security zone has already been configured. If this is not the case, use the following to set up the interface and security zone.

```
admin@SRX# show interfaces ge-0/0/0
description “To Public Ineternet”;
unit 0 {
    family inet {
        address 66.97.23.82/24;
    }
}
admin@SRX# show security zones
security-zone public-inet {
    screen untrust-screen;
    interfaces {
        ge-0/0/0.0;
    }
}
```

7. Add the V10000 “C” port address 172.25.44.19 to the management security zone address book. This step is necessary so that the V10000 can redirect the user Web browser to the “C” port for blocked sites. Note that in addition to the specific address, an “address-set” has also been defined. This was done should the network need to support multiple V10000 appliances. Each additional “C” port would be included in the set, and the associated security policy (in an upcoming step) would not need to be changed.

```
admin@SRX# show security zones
security-zone management {
    address-book {
        address V10000-alpha-c 172.25.44.19/32;
        address-set V10000-c {
            address V10000-alpha-c;
        }
    }
}
```


Copyright © 2010, Juniper Networks, Inc.

8. Create a Websense-specific security application definition for the Websense redirect protocol—TCP/15871.

```
admin@SRX# show applications
application webs-redirect {
    protocol tcp;
    destination-port 15871;
}
```

9. Add a security policy from user-lan to management only to the V10000 “C” port and only for the TCP/15871 traffic. This step is necessary so that the user Web browser can be redirected to the V10000 “Block Page.” Normally User LAN traffic should not be allowed to access the management security zone.

```
admin@SRX# show security policies
from-zone lanA to-zone management {
    policy redirect-only {
        match {
            source-address local-hosts;
            destination-address V10000-c;
            application webs-redirect;
        }
        then {
            permit;
        }
    }
}
```

10. Add any NAT necessary to support both web-redirect traffic as well as user-lan traffic out toward the public Internet.

```
admin@SRX# show security nat source
rule-set websense {
    from zone web-redirect;
    to zone public-inet;
    rule ifnat-all {
        match {
            source-address 192.168.10.0/24;
            destination-address 0.0.0.0/0;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
rule-set user-lan {
    from zone user-lan;
    to zone [ public-inet web-redirect ];
    rule ifnet-all {
        match {
            destination-address 0.0.0.0/0;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
```

Copyright © 2010, Juniper Networks, Inc.

Summary

Juniper Networks SRX Series Services Gateways provide scalable security solutions with Websense TRITON V10000 appliances. This solution is suitable for a wide range of enterprise and service provider customers.

Appendices

Additional information on the SRX Series Services Gateways:
www.juniper.net/us/en/products-services/security/srx-series/

Additional information on Junos OS filter-based forwarding techniques:
www.juniper.net/techpubs/en_US/junos10.2/topics/usage-guidelines/routing-configuring-filter-based-forwarding.html

Additional information on SRX Series security configuration:
www.juniper.net/techpubs/hardware/junos-srx/index.html

Additional general information on Junos OS:
www.juniper.net/techpubs/software/junos/index.html

Additional general information on Junos automation:
www.juniper.net/automation

Additional information about locating Websense security products:
www.websense.com/content/Products.aspx

Additional information regarding installation and deployment of Websense's V10000:
www.websense.com/content/V10000_Support.aspx

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the 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.

8010075-001-EN Aug 2010 Printed on recycled paper

Copyright © 2010, Juniper Networks, Inc.