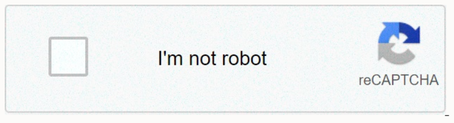

Continue

Juniper firewall guide

To protect a network, a network administrator must create security policies that outline all network resources within that business and the required level of security for those resources. Junos OS allows you to configure security policies. Security rules impose transit traffic rules on what traffic can pass through the firewall, as well as the actions to be performed on traffic as it passes through the firewall. Security policy is a set of reports that control traffic from a specific source to a specified destination by using the specified service. A policy allows, denies or tunnels certain types of traffic one way between two points. Unique name for the rules. From zone to zone, for example: user@host# set security rules from an untrusted zone to a false zoneCovering matching criteria specifying the conditions that must be met in order to apply the policy rule. The matching criteria are based on source IP address, destination IP address, and applications. The user identity firewall provides greater detail, including an additional motorcade, source-identity, as part of the policy statement. A set of actions to be performed in the event of a coincidence – allow, refuse or reject. Accounting and auditing elements – counting, registering or structured registration of the system. If the SRX series receives a package that meets these specifications, it shall perform the action specified in the rules. Security rules impose a set of transit traffic rules, identifying traffic that can pass through the firewall and actions taken on traffic as it passes through the firewall. Traffic actions meeting the specified criteria include permission, rejection, registration or number. For SRX300, SRX320, SRX340, SRX345, SRX380 and SRX550M devices, a default factory security policy is provided that allows all traffic from the trust area to the non-trusted area. Understanding the security policyDo security policy applies security rules for transit traffic in context (from zone to zone). Each policy is uniquely identified by its name. Traffic is classified by matching its source and destination zones, source and destination addresses, and the application that traffic carries in its protocol headers with the policy database in the weeping plan. Each policy is associated with the following characteristics:ZoneA destination zoneOne source or many address names or name addressesOne or many address names of the destination or address set namesOne or many application or application sets, certain namesThis characteristics are called compliance procedure. Each policy also has actions related to it: permission, rejection, number, sign in and VPN tunnel. You must specify match condition arguments when you configure rules, source address, destination address, and application name. You can set yes to with IPv4 or IPv6 addresses using the wildcard record. When flow support is not enabled for IPv6 traffic, all matching IPv4 addresses. When flow support is enabled for IPv6 traffic, all match both IPv4 and IPv6 addresses. To enable flow redirection for IPv6 traffic, use the command to set the inet6 security forwarding option set. You can also set wildcards any-ipv4 or any-ipv6 for the matching criteria of source and destination address to include only IPv4 or only IPv6 addresses, respectively. When IPv6 traffic flow support is enabled, the maximum number of IPv4 or IPv6 addresses that you can configure in the security policy is based on the following compliance criteria: Number_of_src_IPv4_addresses+number_of_src_IPv6_addresses*4<= 1024Number_of_dst_IPv4_addresses+number_of_dst_IPv6_addresses*4 <= 1024Thr reason for the matching criteria is that the IPv6 address uses four times the memory that uses the IPv4 address. Note You can configure security policies with IPv6 addresses only if workflow support for IPv6 traffic is enabled on the device. If you don't want to set a specific app, enter anything as the default app. To search for default applications, from configuration mode, type display groups junos-defaults | (predefined applications). For example, if you don't provide an app name, the policy is installed with the app as a wildcard (default). Therefore, any data traffic that corresponds to the other parameters in a policy will correspond to the policy, regardless of the type of data traffic application. Note: If the rules are configured with multiple apps and more than one of the apps meets traffic, then the application that best meets the matching criteria is selected. The operation of the first policy to be applied to the package. If there are no match rules, the package is dropped. Rules are searched from top to bottom, so it's a good idea to put more specific rules at the top of the list. You should also put IPsec VPN tunneling rules at the top. Place more general rules, such as those that will allow certain users to access all Internet applications, at the bottom of the list. For example, put the reject all or all rules at the bottom after all the specific rules have been analyzed before and legitimate traffic has been enabled count/count/register. Note Support for IPv6 addresses is added in Junos OS version 10.2. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to existing support for active/passive chassis cluster configurations) is added in Junos OS Release 10.4.Policies are considered during stream processing after firewall processing and screens are processed and search is completed by the Service Processing Department (SPU) (for SRX5400, SRX5600 and SRX5800 devices). The reference rules define the destination area, destination address and exit interface. Exit. you create rules, the following rules apply:Security policies are configured in zone-to-zone direction. Under a specific zone direction, each security policy contains a name, match criteria, action, and a variety of options. The name of the rules, the compliance criteria and the action are mandatory. The policy name is a keyword. The source address in the matching criteria is composed of one or more address names or address names in the zone of . The destination address of the matching criteria consists of one or more address names or address names in the zone. The name of the application in the compliance criteria consists of the name of one or more applications or application sets. One of the following actions is required: to allow, deny, or reject. Accounting and auditing elements can be specified: number and journal. You can enable end-of-session logging with the session close command or at the beginning of the session with the session-init command. When the reporting alarm is turned on, set the alarm thresholds in bytes per second or kilobytes per minute. You cannot set global as from zone to zone except for the following condition: All rules configured with a yes zone as a global zone must have one destination address to indicate that either static NAT or incoming NAT is configured in the policy. In the SRX series of service gateways, the policy allowing an option with NAT is simplified. Any optional policy will show whether it allows NAT translation, does not allow NAT translation, or does not care. Address names cannot start with the following saved prefixes. They are only used for the NAT configuration address: static_nat_incoming_nat_junos_Application names cannot start with junos_ reserved prefix. Understanding wildcard addressesSource and destination addresses are two of the five matching criteria that must be configured in security policies. Now you can configure wildcard addresses for the matching criteria of source and destination address in security policy. The wildcard address is presented as A.B.C.D/wildcard mask. The wildcard mask determines which of the bits in IP address A.B.C.D should be ignored by the security policy compliance criteria. For example, the source IP address 192.168.0.11/255.255.0.255 in security policy implies that the criteria for compliance with the security rules may reject the third byte in the IP address (symbolically presented as 192.168.*.11). Therefore, packages with source IP addresses such as 192.168.1.11 and 192.168.22.11 meet the match criteria. However, packages with output IP addresses such as 192.168.0.1 and 192.168.1.21 do not meet the compliance criteria. The use of a replacement address is not limited to entire octets. You can configure any address with a wildcard character. For example, the address of the wildcard 192.168. 7.1/255.255.7.255 that you should ignore only the first 5 bits of the third byte of the replacement address while making the policy for the match. If the use of a replacement address is until full octets, wildcard masks with 0 or 255 in each of the four octets will be allowed. Note: The first octet of the wildcard mask must be greater than 128. For example, a wildcard mask presented as 0.255.0.255 or 1.255.0.255 is invalid. Wildcard security rules are a simple firewall policy that allows you to allow, deny, and reject traffic trying to move from one security zone to another. You do not have to configure security policies using wildcard addresses for services such as Unified Threat Management (UTM). Note Only intrusion and prevention (IDP) for IPv6 sessions is supported for all SRX5400, SRX5600, and SRX5800 devices. UTM for IPv6 sessions is not supported. If your current security policies use wildcard rules, and UTM features are enabled, you will encounter configuration commit errors because UTM features do not yet support IPv6 addresses. To resolve the errors, change the error return rule so that any-ipv4 substitution is used; and create separate IPv6 traffic policies that do not include UTM features. Configuring wildcard security rules on a device affects performance and memory usage based on the number of wildcard rules configured for zone and zone contexts. Therefore, you can configure only a maximum of 480 wildcard policies for zone-specific and zone-specific contexts. Understanding the security policies for traffic-onlySecurity policies are configured on devices to apply traffic services that pass through the device. For example, UAC and UTM policies are configured to apply transitional traffic services. Self-taste or host traffic is incoming for host traffic; i.e. traffic that terminates on the device or outgoing traffic of the host, which is the traffic that is from the device. You can now configure rules to apply services for self-dependent traffic. Services such as the SSL stack service, which must disconnect the SSL connection from a remote device and perform some processing of that traffic, iDP services of incoming traffic, or IPsec encryption of outgoing host traffic must be applied through the security policy configured for standalone traffic. When you configure security rules for self-traffic, traffic passes through the device is first checked against the policy, then against the host incoming traffic option configured for connections associated with the zone. You can configure security rules for self-traffic to apply self-driving services. Outgoing host policy will only work when the package that originates from the host device passes through the stream, and the incoming interface of that package is set to local. The advantages of using a self-driving car are: You can use most of the existing policy infrastructure for the flow used for transit traffic. No separate IP address is required to activate each service. You can apply services or policies to any incoming host traffic with the IP address of the destination of the can configure the security policy only with the relevant services. For example, it is not appropriate to configure the fwauth service on outgoing host traffic, and gprs-gtp services are not associated with the security policy for self-headers. The security policy for self-regulatory traffic is configured in the new default security zone called junos host zone. The Junos-host zone will be part of the default junos configuration so users can delete it. Existing zone configurations such as interfaces, screen, tcp-rst, and host-incoming traffic options are not significant for the junos host zone. Therefore, there is no special configuration for the junos host zone. Note You can use host incoming traffic to control incoming connections to a device; but does not restrict traffic that exits the device. While, junos-reception-zone allows you to select the app of your choice and also limit outbound traffic. For example, services such as NAT, IDP, UTM, and so on can now be enabled for traffic that logs on or out of the SRX Series device using junos-host-zone. View security policy configurationYou must perform the following tasks to create security policy: The Firewall Policy Wizard lets you perform a basic security policy configuration. For more advanced configuration, use the J-Web interface or CLI.Best Practices to determine policies in the SRX Series DevicesA secure network is vital for business. To protect a network, a network administrator must create security policies that outline all network resources within that business and the required level of security for those resources. The security policy applies security rules for transit traffic in the context (zone to zone) and each policy is uniquely identified by its name. Traffic is classified by matching source and destination zones, source and destination addresses, and the application that traffic carries in its protocol headers with the data plan policy database. Table 1 provides policy restrictions for the SRX300, SRX320, SRX340, SRX345, SRX550, SRX650, SRX550M, SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600 and SRX5800. Platform support depends on the version of Junos OS in your installation. Note: Release with Junos OS edition 12.3X48-D15 and Junos OS Release 17.3R1, the maximum number of rule addresses for SRX5400, SRX5600, and SRX5800 devices increased from 1024 to 4096, and the maximum number of context policies increased from 10240 to 80,000.Starting with Junos OS Release 17.3R1, the number of security policies and the maximum number of context policies for SRX5400 , SRX5600 and SRX5800 devices increase from 80,000 to 100,000.Starting with Junos OS Release 15.1X49-D120, the number of policy address objects for the SRX5400, SRX5600, and SRX5800 increases from 4096 to 16,000 table SRX Series Rules Restrictions DevicesSRX DevicesSRX objectsSecurity policiesPolicy contexts (zone pairs)Policies per contextPolicies with counting enabledSRX300SRX3202048128102425610242S6SRX3402048128204851220482S6SRX34520481284096102440962S6SRX3802048128409610244096256SRX550SRX65010241281024020481024010 24SRX550M20481281024020481024010 24SRX1400SRX1500102430721600040961600010 24SRX3400SRX3600409630724000040964000010 24SRX4100102430726000040966000010 24SRX4200102430726000040966000010 24SRX46004096307280000819280000010 24SRX5400SRX5600 SRX58001600030721000008192100000 1024Therefore, as you increase the number of addresses and applications in each rule, the amount of memory that is used by the policy definition increases, and sometimes the system runs out of memory with fewer than 80,000 policies. To get the actual memory usage policy of the packet forwarding machine (PFE) and routing machine (RE), you need to take different components of the memory tree into account. The memory tree includes the following two components: policy context – used to organize all rules in this context. The policy context includes variables such as source and destination zones. Policy Object – used to retain policy data. The policy object calculates memory, such as policy name, IP addresses, address count, applications, firewall authentication, WebAuth, IPsec, number, application services, and Junos services (JSF). In addition, data structures used to store rules, policy sets, and other components use different memory of the packet forwarding machine and the routing machine. For example, address names for each address in the policy are stored in the routing machine, but no memory is allocated to the package forwarding machine level. Similarly, port ranges expand to prefix and masks and are stored in the package forwarding machine, but no such memory is allocated to the routing machine. Memory is also consumed by a deferred deletion state. In a deferred deletion state, when an SRX series device applies a policy change, there is a transient peak usage in which old and new rules are available. So for a short period, old and new policies exist on the package forwarding machine, borrowing memory requirements twice. Therefore, there is no definitive way to clearly determine how much memory is used by a component (package redirection engine or routing engine) at any point in time because memory requirements depend on specific policy configurations and memory is distributed dynamically. The following policy enforcement best practices allow you to make better use of system memory and optimize configuration rules:Use single prefixes for source and destination addresses. For example, instead of using /32 addresses and adding each address individually, use a large subnet that most ip addresses you need. Use the app whenever possible. Each time you define an individual application in the policy, you can use an additional 52 bytes. Use fewer IPv6 addresses because IPv6 addresses consume more memory. Use fewer pairs of zones in policy configurations. Each source or destination zone uses about 16,048 bytes of memory. The following parameters can change the way memory is used by bytes as specified: Firewall – about 16 bytes or more (unfixed) web authentication — about 16 bytes or more (unfixed)IPsec-12 bytesApplication services–28 bytesCount–64 bytesCheck memory usage before and after policy compilation. Note The memory requirement for each device is different. Some devices support 512,000 default sessions, and boot memory is typically 72 to 73 percent. Other devices can have up to 1 million sessions, and charging memory can be up to 83 to 84 percent. In the worst case scenario, to support about 80,000 policies in the SPU, the SPU should start with kernel memory consumption streaming up to 82 percent, and with at least 170 megabytes of memory. Configuring rules by using the Firewall Wizard Firewall Policy Act allows you to perform a basic security policy configuration on SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550M devices. For a more advanced configuration, use the J-Web interface or CLI.To configure rules by using the Firewall Policy Wizard:Select Configure>Tayst>Configure FW Rules in the J-Web interface. Click the Start Firewall Policy Wizard button to start the wizard. Follow the instructions in the wizard. The upper-left area of the wizard page shows where you are in the configuration process. Help that is field sensitive is displayed at the bottom left of the page. When you click a link under the Resources heading, the document opens in your browser. If the document opens in a new section, be sure to close only the tab (not the browser window) when you close the document. Example: Configuring a security policy to enable or deny all trafficThis example shows how to configure a security policy to enable or deny all traffic. RequirementsOverviewConfigurationChasesIn Junos OS, security rules impose transit traffic rules, regarding traffic can pass through the device, as well as actions that need to be performed on traffic as it passes through the device. In terms of security policies, traffic enters one security zone and exits from another security area. In this example, you configure trust and false interfaces, ge-0/0/2, and ge-0/0/1. See Figure 1.Figure 1: Enabling all trafficThis configuration shows how to:Allow or deny all traffic from the the bride zone, but blocks everything from the false area to the trust area. Enable or deny selected traffic from a host in the security zone to a server in a false zone at a specific time. ConfigurationCLI Quick ConfigurationFor quick configuration of this example, paste the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.set security zones security-zone trust interfaces ge-0/0/2 host-inbound-traffic system-services all set security zones security-zone untrust interfaces ge-0/0/1 host-inbound-traffic system-services all set security policies from-zone trust to-zone untrust policy permit-all match source-address anyset security policies from-zone trust to-zone untrust policy permit-all match destination-address any set security policies from-zone trust to-zone untrust policy permit-all match application anyset security policies from-zone trust to-zone untrust policy permit-all then permitset security policies from-zone untrust to-zone trust policy deny-all match source-address anyset security policies from-zone untrust to-zone trust policy deny-all match destination-address anyset security policies from-zone untrust to-zone trust policy deny-all match application anyset security policies from-zone untrust to-zone trust policy deny-all then denyStep-by-Step ProcedureThe following example requires you to navigate various levels configuration hierarchy. For instructions on how to do this, see Use the CLI Editor in configuration mode in the CLI User's Guide. To configure a security policy, to enable or deny all traffic: Configure the interfaces and zones.user@host# set security connections and trust zone ge-0/0/2 host-incoming traffic system services all user@host# set security zone unset dawn interfaces ge-0/0/1 host-inbound-traffic system-services all Create a security policy to allow traffic from the trust zone to not be safe. [Edit zone-to-zone security policy is not true]user@host# set rules allow all match address anyuser@host# rule allow all match address destination every user@host# setting policy allow all matching application anyuser@host # Set rules allow all permitsate security policy to deny traffic from the non-faith zone to the trust zone. [edit zone mistrust policy in zones] user@host# set deny-all rules to match source-address anyuser@host# rules deny all match address anyuser@host# set rules deny-all matching application anyuser@host # set cancel all after denyResultsFrom configuration mode, confirm your configuration by entering show security rules and display commands for security zones. If the output does not show the configuration you want, repeat the configuration instructions in this example to correct it. Note The example configuration is a permission for everyone in the trust area of the Zone. user@host# show the security policy from zone trust to zone distrust {from zone distrust to zone trust {user@host# Show security zones, If you are ready with configuring the device, enter a commit from the configuration Configuration policy To configureverify information about security policy. In ActionFrom Operational Mode, type the Show Detailed Security Policy command to display a summary of all security rules configured on the device. This means that the output displays information about the configured rules in the system. Check the following information: To and from zonesSource and destination addressesSites Clarified: Configuring security rules to enable or deny selected trafficThe example shows how to configure security rules to enable or select traffic. RequirementsOverviewConfigurationChainmentsSa andIndiayu, security rules impose rules on transit traffic, regarding traffic that can pass through the device, as well as actions that need to be performed on traffic as it passes through the device. In terms of security policies, traffic enters one security zone and exits from another security area. In this example, you configure specific security policies to enable only email traffic from a host in the server security zone in an untrusted zone. No other traffic is allowed. See Figure 2.Figure 2: Enable the selected trafficConfigurationCLI Quick ConfigurationTo quickly configure this example, copy the following commands, paste them into a text file, remove all line breaks, change all the data required for your network configuration, copy and paste the commands into the CLI at the hierarchy level [edit], and then type fix from configuration mode.set security zones trust interfaces ge-0/0/2 host-incoming traffic system services all set security zones security zone security zone security-security interfaces ge-0/0/1 host-incoming traffic system-services all set security address book1 address mail unverist 203.0.113.14/24 set security address book1 apply zone unbrossed address for address book 2 mail address -trust 192.168.1.1/32 set security-book address apply address book attachment book setting security rules from zone of distrust of trust in zones policy allow-mail matching mail address mail-trust security rules from zone of trust to zone mistrust policy allow-mail match address of destination mail-infidel setting rules for Protection from zone trust in zone non-wind order allow-mail application for ips settrustru zonetrustru-zone is not at credible levels in the configuration hierarchy. For instructions on how to do this, see Use the CLI Editor in configuration mode in the CLI User's Guide. To configure security rules to enable selected traffic: Configure interfaces and security zones.user@host# set security-zone trust interfaces ge-0/0/2 host-incoming traffic system services all user@host# set security zone unobtrusive interfaces ge-0/0/1 system-services all Create address records for the client and server. Also apply security zones to address books. [edit security book1] user@host# mail address non-faithful 203.0.113.14/24 user@host# apply zone is not true [edit address book2]user@host# mail address 192.168.1.1.1 user@host# apply zone trust Give mail rules. [edit security policy from zone to zone is not true]user@host# setting rules allow-mail matching mail address-trustuser@host# rules allow mail match address to unobtrusive user@host# setting rules allow matching application junos-mail user@host# set policy allow e-mail then Enable configuration from mode, confirm your configuration by entering display security policy and display security zones commands. If the output does not show the scheduled configuration, repeat the configuration instructions in this example, to correct it.user@host# show security policy from zone trust to zone non-aligned {mail address;destination mail address is not true;user@host# show security zonesuser@host# show display zonesuser@host# show display of security address-bookaddress mail-false 203.0.113.14/24;mail-trust address 192.168.1.1/32;If you are ready to configure the device, configuration mode. VerificationVerifying configuration policyPurposeVerify security policy information. In ActionFrom Operational Mode, type the Show Detailed Security Policy command to display a summary of all security rules configured on the device. This means that the output displays information about the configured rules in the system. Check the following information: To and from zonesSource and destination addressesSites Clarified: Configure security policy to enable or deny to address trafficThis example shows how to configure security rules to enable or deny replacement address traffic. RequirementsOverviewConfigurationChasionsOptions in Junos OS, security rules impose rules on transit traffic, regarding traffic that can pass through the device, as well as actions that need to be performed on traffic as it passes through the device. In terms of security policies, traffic enters one security zone and exits from another security area. In this example, you configure specific security to allow only wildcard address traffic from a host in the Trust zone to a false zone. No other traffic is allowed. ConfigurationCLI Quick ConfigurationFor quickly configure this example, copy the following commands, paste them into a text file, remove all line breaks, change all data required for your network configuration, copy and paste the commands into the CLI at hierarchy level [edit], and then type perform in configuration mode.set security zones trust interfaces ge-0/0/2 host-in System Services to connect to all specified security zones non-return interfaces ge-0/0/1 host-inbound-traffic all specified security address-book1 address wildcard-trust-address 192.168.0.11/255.255.0.255 set security address connect zone trust set security policy from zone trust to zone mistrust rules allow-substitute matching source-substitute security code from security zone to zone non-privacy way to access zone non-faith way-replace address address any address protection from zone trust to zone mistrust policy allow-substitute matching application anyset security rules from zone trust to zone mistrust policy allow-substitution then allow step-by-step procedureThen, the example requires you to navigate different levels in the configuration hierarchy. For instructions on how to do this, see Use the CLI Editor in configuration mode in the CLI User's Guide. To configure security rules to enable selected traffic: Configure interfaces and security zones.user@host# set security-zone trust interfaces ge-0/0/2 host-incoming traffic system services all user@host# set security zone untrusted interfaces ge-0/0/1 host-inbound-traffic system-services all Create address for host and attach address book to zone. [edit security ledger address1] user@host# set the wildcard address to a credible address 192.168.0.11/255.255.0.255 user@host# set to security zone thick under the rule to allow wildcard address traffic. [editing security policy from zone to zone is not true]user@host# setting rules allow-substitute match-source-substitute-trustuser@host# rules permit-wildcard matching destination address-address anyuser@host# setting permit-wildcard rules anyuser@host matching application permit-commands set policy permit-wildcard allow wildcard configuration mode, confirm your configuration by entering security display rules and displaying security commands zones. If the output does not display the configuration you want, repeat the configuration instructions in this fix example it.user@host# show security policies from doson trust in false {security source address;user@host# show zonesuser@host# show address-book security address 192.168.0.11/255.255.255;If you are done configuring the device, configuration mode. VerificationVerifying configuration policyPurposeVerify security policy information. In operational mode, type the command to display the security policy name of the replacement permission to display details of the wildcard security policy configured on the device. Which means the Magnifier displays information about the wildcard permission rules configured in the system. Check the following information: From and to zonesSource and destination addressesSitesRequires: Configuring rules to protect traffic redirection to a server for external system LogThis example shows how to configure security rules to send a path registered on an external server system log server. RequirementsOverviewConfigurationSysese example uses the following hardware and software components: Client connected to device SRX5600 in the ge-4/0/5A server interface connected to the SRX5600 in the ge-4/0/1Folds generated on the SRX5600 device are stored on a Linux-based system logging server. Before you configure this feature, an SRX5600 device connected to the Linux server is required when a ge-4/0/4No interface requires a special configuration beyond the initialization of the device. In this example, you can configure security policies on an SRX5600 device to send traffic logs generated by the device during data transmission to a Linux-based server. Traffic logs record details for each session. Log files are generated during the session to establish and terminate between the source and destination drive that are associated with the SRX5600 device. ConfigurationCLI Quick ConfigurationFor quickly configure this example, copy the following commands, paste them into a text file, remove all line breaks, change all the data required to match your network configuration, copy and paste commands into CLI at the hierarchy level [edit], and then type Perform in the error configuration.set security registry source-address 127.0.0.1set security log flow trafficlogs acuity debug set security logon flow traffic host host 203.0.113.2 sets security security zones security on client host-traffic host-traffic all set security zones for client host-zone host-zone client for incoming traffic protocols all specified security zones client security interfaces-4/0 /5.0 Set security zones for security server host-server for incoming traffic-traffic system services all certain security security zones -zone server interfaces on the server ge-4/0/4.0 server set security zones server interfaces on the ge-4/0/1.0 server set security rules from client to zone server matching source address of all specified client security for zone The server matching of each set of security policy from client to zone synchronization compliance policy of all specified security rules from the client zone to the zone server allow then set the security policy to zone security rules from the client zone to the zone server matching after you log on to session-init security rules from the client zone in zone server rules matching then log the procedure to close the session step by step The following example requires you to navigate different levels in the configuration hierarchy. For instructions on how to do this, see Use the CLI Editor in configuration mode in the CLI User's Guide. To configure the security policy to send logs to an external system log server: Configure the security logs for traffic log transfer generated in the SRX5600 device on an external system log server with IP address 203.0.113.2. IP address is the return address of the SRX5600 device. user@host# Set source-address 127.0.0.1user@host# set trafficlogs flow severity debug user@host# set stream trafficlogs host 203.0.113.2 Configure security zone and specify types traffic and protocol they are enabled for interface ge-4/0/5.0 of SRX5600 device.user@host# sets security zone client host-incoming traffic system services all clients user@host# set security zone client protocols all user@host# defined security client interfaces and zone ge-4/0/5.0 Configuring another security zone and determines the types of traffic that are enabled on the ge-4/0/4.0 and ge-4/0/1.0 interfaces of the SRX5600 device.user@host SRX5600 <3> <0># set security zone server host-in-traffic system-services all user@host# set security zone server interfaces ge-4/0/4.0 user@host# set security interfaces and zone server ge-4/0/1.0 Create a policy and specify compliance with the criteria for this policy. Compliance criteria indicate that the device can allow traffic from any source to any destination and for any app. [edit client-to-zone security policy server] user@host# policy set match the address of the destination address every user@host# match set application every user@host# rule matching then allow each Enable traffic data logging policy at the beginning and end of the session. [edit security policy from client zone to zone server] user@host# Match policy set then log session-init user@host# match policy set then log session Close ResultsFrom configuration mode, confirm the configuration by typing the show security log command. If the output does not show the configuration you want, repeat the configuration instructions in this example to correct it.user@host# show logsource-security address 127.0.0.1;If you are ready to configure the device, type a commit from configuration mode. VerificationCon has confirmed that the configuration is working correctly. Check zonesVerifying policiesVerifying zonesSaving Versverge that the protection zone is enabled or not. ActionFrom operational mode, type the Show Security Zones command. Check the rules ForpurpositionVery that the rules work. In ActionFrom operational mode, type the Show security policy command on all devices. Terminal Access Point (TAP) mode for security zones and rules allows you to passively monitor traffic flows over the network via a SPAN switch or mirror port. Terminal Access Point (TAP) mode is a standby device that checks mirror traffic using a switch. If security zones and policies are configured, TAP mode checks incoming and outgoing traffic by configuring the tap interface and generating a security log report to show the number of threats detected and user usage. If some packages are lost in the crane interface, the zones and security policy terminates the connection, as a result of which no report generates this connection. The security zone and policy configuration remain the same as tap mode. When you configure an SRX series device to run in NRA mode, the device generates security log information for the information about threats detected, use of applications and user data. When the device is configured to run in TAP mode, the SRX series device receives packages only from the configured TAP interface. In addition to the configured TAP interface, other interfaces are configured interface or connected to the external server. The SRX Series device will generate a security report or log in according to incoming traffic. The security policy will also be configured by default after the TAP interface is configured. You can configure other zones or rules if necessary. If an interface is used to connect a server, then the IP address, routing-interface, and security configuration must also be configured. Note You can configure only one TAP interface when working with the device in TAP mode. Example: Configuring security zones and policy areas in TAP modeThis example shows how to configure security zones and rules when the SRX device is configured in TAP (terminal access point) mode. RequirementsOverviewConfigurationConfidenceConfidenceThis example uses the following hardware and software components: SRX series deviceJunos OS Release 19.1R1OverviewIn this example, you can configure the SRX series device to run in TAP mode. When you configure an SRX series device to run in NRA mode, the device generates security log information to display information about threats detected, using applications, and user data. ConfigurationCLI Quick ConfigurationFor quick configuration of this example, copy the following commands, paste them into a text file, remove all line breaks, change all details needed to match your network configuration, and copy and paste the commands into the CLI level of the [edit] hierarchy level, and then type execution from configuration mode. setting security zones tap-zone interfaces ge-0/0.0set security zones security zones tap-zone tap-zone tap-zone trackingset application trackingset set of security rules from tap-zone to tap-zone policy tap-zone match source-address of all security rules from tap-zone to-zone tap-zone policy tap-zone match destination - address of any set of security rules from tap-zone tap-zone -zone tap-policy match application all set security rules from tap-zone tap-zone tap-zone crane-rules then enable initial security rules from tap-zone to tap-zone crane-zone crane-zone-then log session-initset security rules from tap-zone tap-zone to tap-zone crane-policy after log session-closeStep-by-step ProcedureThen requires you to navigate different levels in the configuration hierarchy. For instructions on how to do this, see Use the CLI Editor in configuration mode in Junos OS CLI User Guide.To configuring zones in TAP mode: Configuring the tap-zone security zone interface.user@host# certain security zones security zone tap-zone tap-zone interfaces ge-0/0/0.0Configure security zone tap-zone tap-zone tracking.user@host # defines security zones security zone tap-zone tap-zone trackingConfig security policy that allows traffic from zone tap-zone tap-zone crane zone policy and configure matching condition.user@host# certain protection rules from tap-zone tap-zone tap-zone tap-policy match source-address-address anyuser@host# set protection protection from tap-zone tap-zone tap-zone tap-policy match destination - address anyuser@host# certain security rules from tap-zone to tap-zone tap-zone tap-zone tap-zone match application anyuser@host# set protection rules from tap-zone tap-zone tap-zone rules tap-zone then permituser@host # Set security Rules from tap-zone to tap-zone tap-zone crane-rules then log session inituser@host# set security rules from tap-zone to tap-zone crane-zone crane-rules then log session-closeResultsFrom configuration mode, confirm configuration, by entering show security zones and displaying the security policy commands. If the output does not show the configuration you want, repeat the instructions in this example to correct configuration.user@host zonesuser@host#show tap-zone protection rules to tap-zone {If you are ready to configure the device, enter a commit from configuration mode. Check To make sure the configuration is working correctly, perform the following tasks: Check the policy configuration in TAP ModePurposeVerify security policy information. ActionFrom operating mode, enter the details of the security command.user@host > display security policy details: -- default policy: Enable all pre-ID rules: Enable All Rules: Trust_to_Untrust, Action: Permission, Status: Enabled, Index: 4, Scope Rules: 0 Policy Type: Configured Sequence Number: 1 of Zone: izone, For Zone: Ozone Addresses: All ipv4 (Global): 0.0.0/0 any-ipv6 (global): ::/ 0 Destination addresses: any-ipv4 (global): 0.0.0.0/0 any-ipv6 (global): ::/0 Application: each IP protocol: 0, ALG: 0, Timeout: 0 Output port range: [0-0] Destination port range: [0-0] rules TCP options: SYN check: No, SEQ check: no, window scale: No session log: when creating, at closer policy: Untrust_to_Trust, Action type: Permission, Status: Enabled, Index: 5, Scope Policy: 0 Policy Type: Sequence Number: 1 of Zone: o , To Zone: izone Source Addresses: any-ipv4 (Global): 0.0.0/0 any-ipv6 (global): ::/ 0 Destination addresses: any-ipv4 (global): 0.0.0.0/0 any-ipv6 (global): ::/0 Application: each IP protocol: 0, ALG: 0, Idle timeout: 0 Output port range: [0-0] destination port range: [0-0] of TCP options rules: SYN validation: no, SEQ check: no, window scale: No session log: when-create, in-close MeaningDisplays summary of all security rules configured on the device in tap mode. Dynamic address groups in security policyRight-add address entries to a policy may take a long time. There are external sources that provide lists of IP addresses that have a specific purpose attribute (such as a specific location or behavior that may pose a threat). You can use the external source to identify threat sources by their IP address, then group these addresses into a dynamic address record, and of this entry in a security policy. This way, you can control traffic to and from these addresses. Each such group of IP addresses is called a dynamic address record. The following types of IP addresses are supported: one IP. For example: 192.0.2.0IP range. For example: 192.0.2.0- 192.0.2.10CIDR. For example: 192.0.2.0/24 Each record occupies one line. Starting with Junos OS Release 19.3R1, IP address ranges should not be sorted in ascending order, and the value of IP records may overlap in the same file. In Junos OS editions before 19.3R1, IP address ranges must be sorted in ascending order, and the value of ip records cannot overlap in the same feed file. Note A dynamic address record is a group of IP addresses, not an IP prefix. The dynamic address record differs from the security address concepts of address books and address entry addresses. The following are the advantages of deploying dynamic address records in security policy: a network administrator has more control over traffic to and from groups of IP addresses. The external server provides an updated IP address channels to the SRX series device. The administrator's efforts have been drastically reduced. For example, in an old security policy configuration, adding 1,000 address records for a reference policy will require about 2,000 configuration lines. By defining dynamic address recording and referencing in a security policy, up to millions of records can be insuffered into the SRX Series device without much additional configuration effort. No commit process is required to add new addresses. Adding thousands of addresses to a configuration using a legacy method takes a long time for a commit. Alternatively, ip addresses in a dynamic address record come from an external channel, so a commit process is not required when the addresses in a record change. Figure 3 illustrates a functional overview of how the dynamic address record works in security policy. Figure 3: Functional components of the dynamic address record in security policyFor security security refers to the dynamic address record in the source or destination address field (in the same way that security rules refer to the legacy address record). Figure 4 illustrates a policy that uses a dynamic address record in the Destination Address field. Figure 4: Dynamic address entry in security policyIn Figure 4, Policy 1 uses the destination address 10.10.1.1, which is a legacy security address record. Policy 2 uses the destination address vendor list that is a dynamic address record named by the network administrator. Its contents are the list of IP addresses retrieved from an external feed file. Packages that meet all five criteria (from zone name is not true, zone name engineer, any source address, destination IP address that belongs to the vendor block list dynamic address, and mail application) are processed which are to refuse and register a package. Note: Note: address record names share the same space name as legacy security address records, so do not use the same name for more than one record. The Junos OS execution process checks that the names are not duplicated to avoid conflict. Dynamic address groups support the following data feeds: Custom lists (whitelists and blacklists)GeoIPFeed ServersBundle FeedsIP addresses, IP prefixes, or IP ranges contained in a dynamic address record can be updated periodically by downloading an external feed. SRX series devices periodically start a connection to the channel server to download and update IP lists that contain the updated dynamic addresses. Starting from Junos OS Release 19.3R1, you can download a single tgz file from the server and extract it into several children's feed files. Each individual file corresponds to one feed. Let the individual dynamic addresses refer to the feed in the package. The batch file reduces overhead CPU when too many feeds are configured, where multiple child feeds are compressed into one .tgz file The following batch feed modes are supported: Archive File ModeArchive ModeArchiveIn backup mode, you must compress all feed files for the SRX Series device into one tgz file. The SRX Series drive downloads this file and retrieves all feeds after retrieval. This process is explained below: When the feed server URL is the URL of a .tgz suffix file instead of the original URL of the folder, it means that that server uses one file to carry all its channels to deploy the dynamic SRX Series address. In this scenario, the feeds under this server inherit the refresh interval or retention interval from the server. Any user configuration of the update interval or retention interval for this feed is ignored. After this change, follow the steps below to support server feeds as shown below. The example below shows the steps required to maintain server feeds:Insert all feed files for the SRX series device under the folder feed-4-srxGenerate all files to submit fd1 fd2 fd3 .. fdN in the feeds-4-srxAdd folder or remove IP ranges from channelsProven the files by running the following command: cd feeds-4-srx;tar -zcvf .. /feeds-4-srx.tgz*;cd-Post step 4, the file powered-4-srx.tgz is ready to download the SRX series drive containing the same folder that contains the feeds-4-srx.tgz file. After downloading, extracted files are placed in the same folder as feeds-4-srx.tgz. The following example shows the configuration of the SRX Series device: Set the security dynamic address information server server-4-srx URL 10.170.40.50/feeds-4-srx.tgzset security dynamic address feed-server server-4-sr Feed-name feed1 feed path fd1set security dynamic address Server Server-4-srx feed-name feed2set protection dynamic address information server 4-srx channel-channel name 3 path fdN Path parameter requires the relative flow path in the connection archive. If tar -zxf feeds-4-srx.tgz generates feed folder-4-srx and this folder contains a submission file use the command below to configure feed:set security dynamic address information server server-4-srx channel fd1 time feeds-4-srx/fd1If tar -zxf feeds-4-srx.tgz retrieves the file directly fd1 file, then use the following command to configure the feed:setting the security dynamic address of the server-server-4-srx feed fd1 time fd1Flat File ModeFlat file mode offers maximum simplicity for the user by entering a single syntax change in the existing file feed format. The content of all feed files is collected in one file, with .bundle as a suffix. This allows you to manage a single file. The SRX Series drive classifies IP ranges in this package file into multiple emission files. You can gzip this file as .bundle.gz if you can save some bandwidth. In addition to the file format defined above, enter a feed uppercase label: followed by the channel name. The lines below this label are considered to be IP ranges belonging to the feed. An example of the appearance of the file format is given below: root@st;as feeds-4-srx.bundleConfiguration configuration of an SRX series drive is similar to backup mode and is given below: set the security dynamic address of feed-server server-4-srx URL 10.170.40.50 /feeds-4-srx.bundleset protection dynamic-address feed server server-4-srx channel name fd1 time fd1set security dynamic address information server server-4-srx name fd2 time fd2 time fd2 The difference between flat mode and backup mode is file suffoth and inside file layout. You can choose the most convenient mode for you. Because feed files are in plain text format, gzip can reduce the file size. If a server and an SRX Series device has WAN link in between, use a smaller sized file to be transmitted on the network, in this case, gzip the bundle file and configure the following commands:set security dynamic-address feed-server server-4-srx url 10.170.40.50/feeds-4-srx.bundle.gzset security dynamic-address feed-server server-4-srx feed-name fd1 path fd1set security dynamic-address feed-server server-4-srx feed-name fd2 path fd2Feed Server Support for SRX Series DevicesTable 2: PlatformMaximum Number of Feed ServersMaximum Number of FeedsMaximum Number of Dynamic Addresses entriesSRX300SRX320SRX340SRX345SRX550SRX550MSRX65010500500SRX4100SRX4200SRX4600SRX5400SRX5600SRX5800vSRXvSRX 3.010050005000SRX15004020002000Starting with Junos OS Release 17.3R1, the number of security policies and the maximum number of policies per context for SRX5400, SRX5600, and SRX5800 devices increases from 80,000 to 100,000.Starting with Junos OS Release 15.1X49-D120, the number of address objects per policy for SRX5400 , SRX5600 and SRX5800 increased from 4096 to 16,000.Starting with Junos OS Release 12.3X48-D15 and Junos OS release 17.3R1, the maximum number of policy address objects for SRX5400, SRX5600, and SRX5800 devices increases from 1024 to 4096, and number of context policies increases from 10240 to 80,000.Support for IPv6 addresses in active/active chassis cluster cluster (in addition to existing support for active/passive chassis cluster configurations) in Junos OS Release 10.4.Support for IPv6 addresses is added in Junos OS version 10.2. 10.2.