iNET ZERO

your JNCIE training partner

iNET ZERO - JNCIE-SEC

Lab Preparation workbook

V1.3 (2017)

For Juniper Networks ® - JNCIE-SEC 2017 Lab exam

Copyright and licensing information

ISBN/EAN

978-90-819227-0-8

About iNET ZERO's content developers and authors:

Alexey Kolmov

Alexei lives in Moscow and speaks Russian and English. He started his carrier in telecommunication area in 1995 as a technician in S.W.I.F.T. Access Point. Since that time he gained experience as a field, technical support and systems engineer, project manager, technical writer and instructor. He had taken part in many projects for corporate clients and service providers, participated in the creation of networks based on X.25, Frame Relay, ATM, PDH/SDH, TCP/IP and VoIP technologies, learned and implemented solutions from Motorola, Nortel Networks, Tellabs and Acme Packet.

Since 2006 Alexei has been working with Juniper Networks technologies and products, focusing primarily on security solutions. Alexei becomes energized and determined to stimulate people to move, grow and develop to higher levels of personal effectiveness. Alexei holds the following certification: JNCIE-SEC#113, JNCIP-M/T, JNCIS-FW, JNCIS-SSL, JNCIA-EX and Acme Packet Certified Instructor

Richard Pracko

Richard Pracko comes from the heart of the Europe, from a small but beautiful country Slovakia. Right after finishing his studies at the university with telecommunications as a major, he joined the Siemens Networking department, and focused on the integration of Juniper Networks and Siemens products. There, he gathered a lot of experience and skills in the networking area by taking an active part to numerous projects, and this , all over the world. It was during that time that his teaching career started. In the beginning of 2009, he left Siemens on his own initiative, and became a full time instructor and technical consultant, over a vast geographic area (EMEA and more).

Richard is an energetic young man, with interests ranging across numerous sport disciplines like tennis, soccer, skiing and others. Richard speaks English, German, Czech and Slovak. Richard holds the following certifications: JNCIS-FWV, JNCIP-SEC, JNCIS-ENT, JNCIA-EX.

Jörg Buesink

Jörg lives in the Netherlands near Amsterdam and brings more than 10 years of experience in the IT and networking industry. He has worked for several large ISPs / service providers in the role of technical consultant, designer and network architect. He has extensive experience in network implementation, design and architecture and teached several networking classes. Jörg is Huawei HCIE, triple JNCIE certified (JNCIE-ENT#21, JNCIE-SP#284 and JNCIE-SEC#30) as well as triple CCIE#15032 (Routing/ Switching, Service provider and Security) and Cisco CCDE#20110002 certified.

Rack rental service

Did you know that this workbook can be used in combination with our premium JNCIE rack rental service? Take a look on our website for more information www.inetzero.com

Warning:

Please do NOT change the root account password for any of our devices to prevent unnecessary password recovery. Thank you for your cooperation

Target audience

This workbook is developed for experienced network engineers who are preparing for the Juniper Networks JNCIE-SEC lab exam. Although not required it is highly recommended that you have passed the JNCIS-SEC and JNCIP-SEC written exams before you start using this workbook. iNET ZERO's JNCIE-SEC preparation workbook is developed in such a way that we expect you to have theoretical knowledge about the JNCIE-SEC lab exam blueprint topics (JNCIP-SEC certified or working towards this certification). For example, in this workbook we will not explain what route-based VPNs, UTM and NAT are. What we will do is test if you are able to configure all these technologies based on certain requirements and understand how they interact in a typical SEC environment.

How to use this workbook

We recommend that you start your JNCIE lab preparation with the workbook chapters only. Always take a note on the time spent for each chapter/ task to see if you improved once you go over the chapters again. Ensure that at least you go the workbook chapters twice before you start with the super lab. You are ready to try the Super Lab if you are able to configure the chapters tasks without the need of the chapters answers.

iNET ZERO support

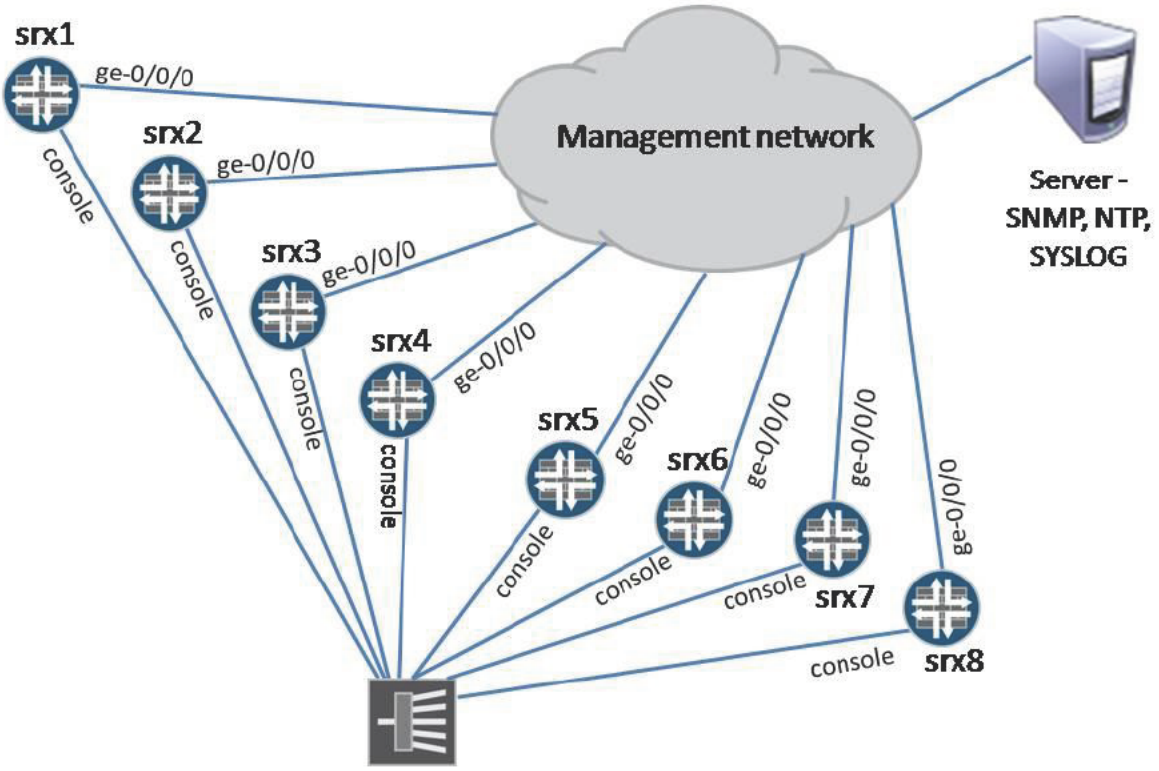
Always feel free to ask us questions regarding the workbook or JNCIE rack rental. You can reach us at info@inetzero.com. We love to hear from you regarding your preparation progress. Your feedback regarding our products is also very appreciated!

Table of Contents

Chapter one: General system features

This chapter focuses on initial system configuration and general system features. You will configure various features, such as hostnames, access to the management network, authentication and authorization, ntp, snmp and syslog.

Topology for chapter one:



NOTE:

Always verify if you have the latest initial configurations on our website (due to possible updates):http://www.inetzero.com/pics/wb/sec/wb-configs-secv12-latest.zip If you do not have the latest version of the configuration files you can request the configs by sending an email to **info@inetzero.com**, including your order receipt.

Load the configs on the lab devices. Ensure that you do not forget to load the infrastructure configurations for the switches (vr-device and the access switch).

TIP: Ensure you read this entire chapter, before starting with the first task.

Task 1: Initial configuration

In this part you will configure the device hostnames, the management network interface details including definition of specific services allowed for accessing the device.

1) Configure the hostnames on the devices according the table below:

device	Hostname
device1	srx1
device2	srx2
device3	srx3
device4	srx4
device5	srx5
device6	srx6
device7	srx7
device8	srx8

2) Based on the topology diagram configure the management and loopback interfaces on each device with the IP address as listed in the table below:

Device	Management IP address	Loopback IP address
srx1	10.10.1.1/24	192.168.1.1/32
srx2	10.10.1.2/24	192.168.1.2/32
srx3	10.10.1.3/24	192.168.1.3/32
srx4	10.10.1.4/24	192.168.1.4/32
srx5	10.10.1.5/24	192.168.1.5/32
srx6	10.10.1.6/24	192.168.1.6/32
srx7	10.10.1.7/24	192.168.1.7/32
srx8	10.10.1.8/24	192.168.1.8/32

3) The management interface on each device needs to be used purely only for management access and won't accept any transit traffic. In addition this interface will accept only specific services as defined in the table below:

Device	Hostname
srx1	ssh with allowed root access, telnet, http, https
srx2	ssh with allowed root access, telnet, http, https
srx3	ssh with allowed root access, telnet, http, https
srx4	ssh with allowed root access, telnet, http, https
srx5	ssh with allowed root access, telnet, http, https
srx6	ssh with allowed root access, telnet, http, https
srx7	ssh with allowed root access, telnet, http, https
srx8	ssh with allowed root access, telnet, http, https

Ensure the listed services are enabled.

4) Limit the number of SSH connections to maximum 5 per minute. This limitation is also valid for telnet.

Task 2: Authentication and authorization

In this part you will configure new users allowed to access the devices and define their privileges and permissions.

1) On every device create a new user **lab** with the password **lab123** that will have super-user privileges.
2) Configure the following additional users on the devices as defined in the table below:

Username	Password	Device	Privileges
ronly	ronly123	All	Has permissions"view" and "view-configuration". Additionally can NOT execute the "file delete" command.
admin1	admin123	All	Has permissions "all". Can access the configuration mode only using "configure private" command.
restricted	restricted123	All	Has permissions "clear" and execute only the "show system uptime", "show system storage" and "show interfaces terse" commands and nothing else.

-

Task 3: Syslog

1) Ensure that all deviceshave following SYSLOG configuration:
   a. All “emergency” messages regardless of the facility are displayed on terminals of all currently logged users.
   b. All messages regardless of the facility with the severity of “critical” and higher are sent to the default syslog file.
   c. A file named “interactive-commands” with command audit trail is maintained, i.e. file with records about the users and commands they execute.
   d. A separate file named “security-policy-logs” is used for security policy log entries. The system should retain 20 archive files each with size of 512 KB (524288 B).
   e. A separate file named “authorization-file” is used for authorization messages with the severity “info” and higher.
   f. All “emergency” messages regardless of the facility are sent to the syslog server at 10.10.10.2. Additionally use a non-physical address as source address for the syslog messages.
   g. Ensure the information about the year is included in these messages.

Task 4: NTP

1) Ensure that all devices synchronize their time with a NTP server reachable at 10.10.10.3. Additionally use a non-physical address as source address.
2) On all devices set the time zone to Europe/Amsterdam.
3) The srx1, srx2 and srx8 should use the MD5 authentication with the key number 1 and the password set to "**bootcamp**" for ntpserver and should only accept ntp updates using the same phrase.
4) On srx7 configure a second ntp server (10.10.10.6) which should be used in case the server from step 9) is not available.
5) The srx5 device should use only ntp messages authenticated with key number 5 and key value "**ntpserver**". However the ntp messages send out of the deviceshould not contain any authentication.

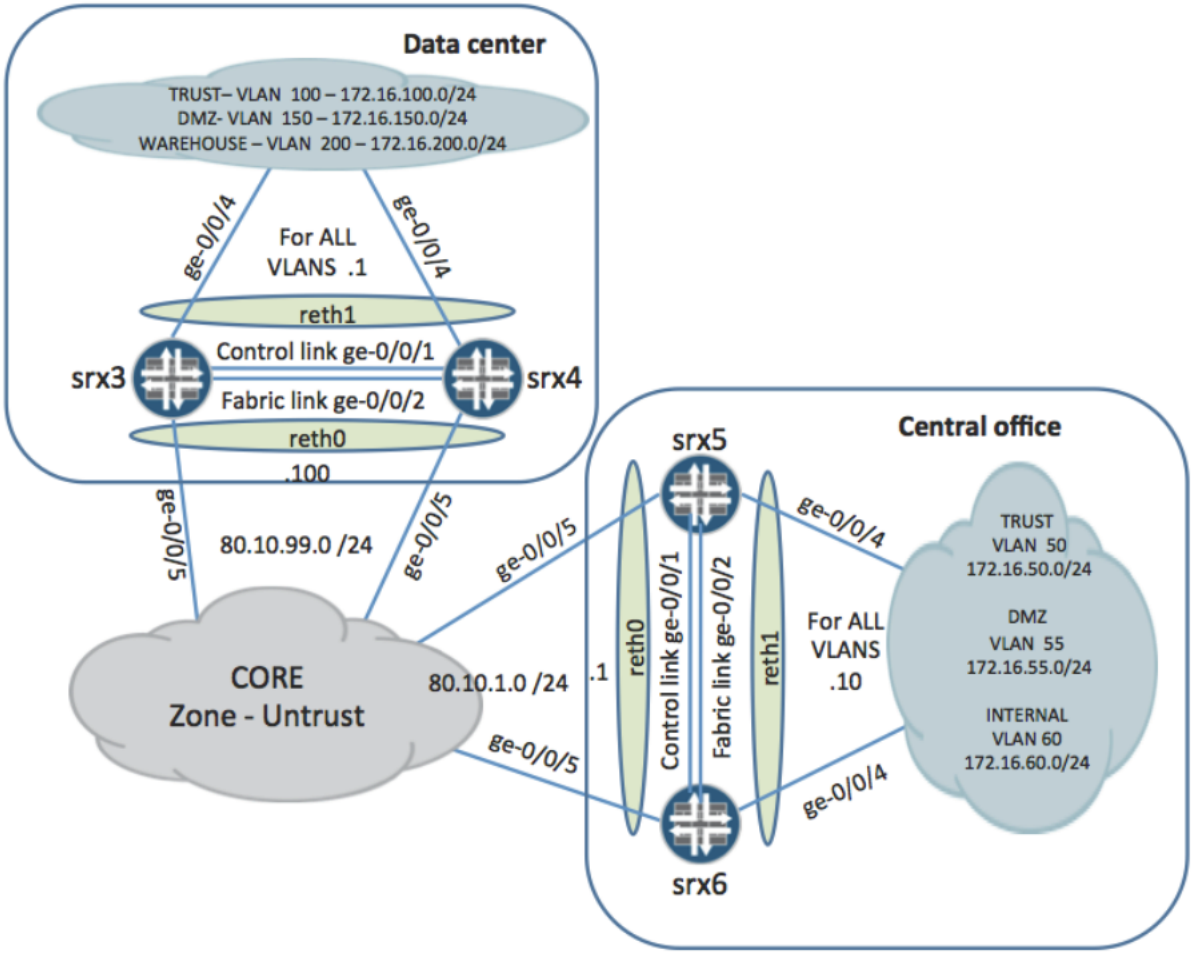
Task 5: SNMP

1) Configure all devices to accept read-only snmp requests only from the NMS system located at 10.10.10.4 using the community string "**reading**".
2) Configure all devices to send the following snmp traps to the NMS system:
    a. Authentication failures
    b. Hardware and environment
    c. Link transitions
    d. Routing protocol
3) The srx1 should send notifications about link transitions to a specific monitoring system reachable at 10.10.10.5. Thespecific monitoring system listens on the port 5999 for traps and understands only SNMP version 1.
4) The srx8 should accept also read-write requests from the network 2.2.2.0/28 but the following two IP addresses 2.2.2.5 and 2.2.2.10 are excluded. The community string is "**snmpRWaccess**".
5) On srx1 and srx2define the SNMP contact, description and location with "**Adminuser**", "**JNCIE-SEC device**" and "**Amsterdamrack**" respectively. In addition define the system location (not in the SNMP configuration) with following values: rack number 1, floor 1.

Chapter two: High availability

This chapter focuses on high availability on the SRX devices, i.e. clustering. You will create two SRX clusters and configure them, including control and fabric links, redundancy groups (RG) and their parameters, and redundant Ethernet interfaces (reth).

Topology for chapter two:



You can continue with the configuration in case you have completed tasks from the previous chapter. OR load the latest initial configurations for this chapter.

NOTE: In case you have already loaded the initial configuration for the switches (vr-device and access switch) before you don't have to do it again.

TIP: Ensure you read this entire chapter, before starting with the first task.

Task 1: Creating clusters – initial setup

In this part you will create 2 clusters.

1) Create clusters as defined in the table below:

Device	Node id	Cluster id
srx3	0	1
srx4	1	1
srx5	0	2
srx6	1	2

2) Ensure that both clusters use the ge-0/0/1 as the control link and ge-0/0/2 as the fabric link. Additionally configure automatic reboot of disabled node after control link failure recovery.
3) Configure each node in both clusters with the hostname and management IP address according to the table below:

Cluster-id/Node-id	Hostname	Management IP address
1/0	srx3	10.10.1.3/24
1/1	srx4	10.10.1.4/24
2/0	srx5	10.10.1.5/24
2/1	srx6	10.10.1.6/24

The loopback addresses for the clusters are as follows:

Cluster-id 1: 192.168.1.3/32
Cluster-id 2: 192.168.1.5/32

Task 2: Configuring redundancy groups and redundant ethernet interfaces

Here you will create redundancy groups (RG) and define their parameters, configure redundant ethernet interfaces (reth) and associate them with the redundancy groups.

1) Ensure the node 0 will be the primary for the routing engine RG on both clusters.
2) Configure redundant ethernet interfaces on both clusters as depicted on the topology image.
3) On cluster-id 1 (cluster 1):
    a. Configure RGs in a manner that allows the defined reths to failover independently of each other.
    b. If multiple RGs are needed to satisfy the previous requirement configure them to be always equally distributed among the nodes, i.e. if both nodes are available each node will have always active half of the RGs.
    c. Ensure each child interface failure triggers RG failover.

4) On cluster-id 2 (cluster 2):
    d. Configure RGs in a manner where all reths will be active always on the same node.
    e. There is no need to RGs failback after failure recovery.
    f. Ensure each child interface failure triggers RG failover.

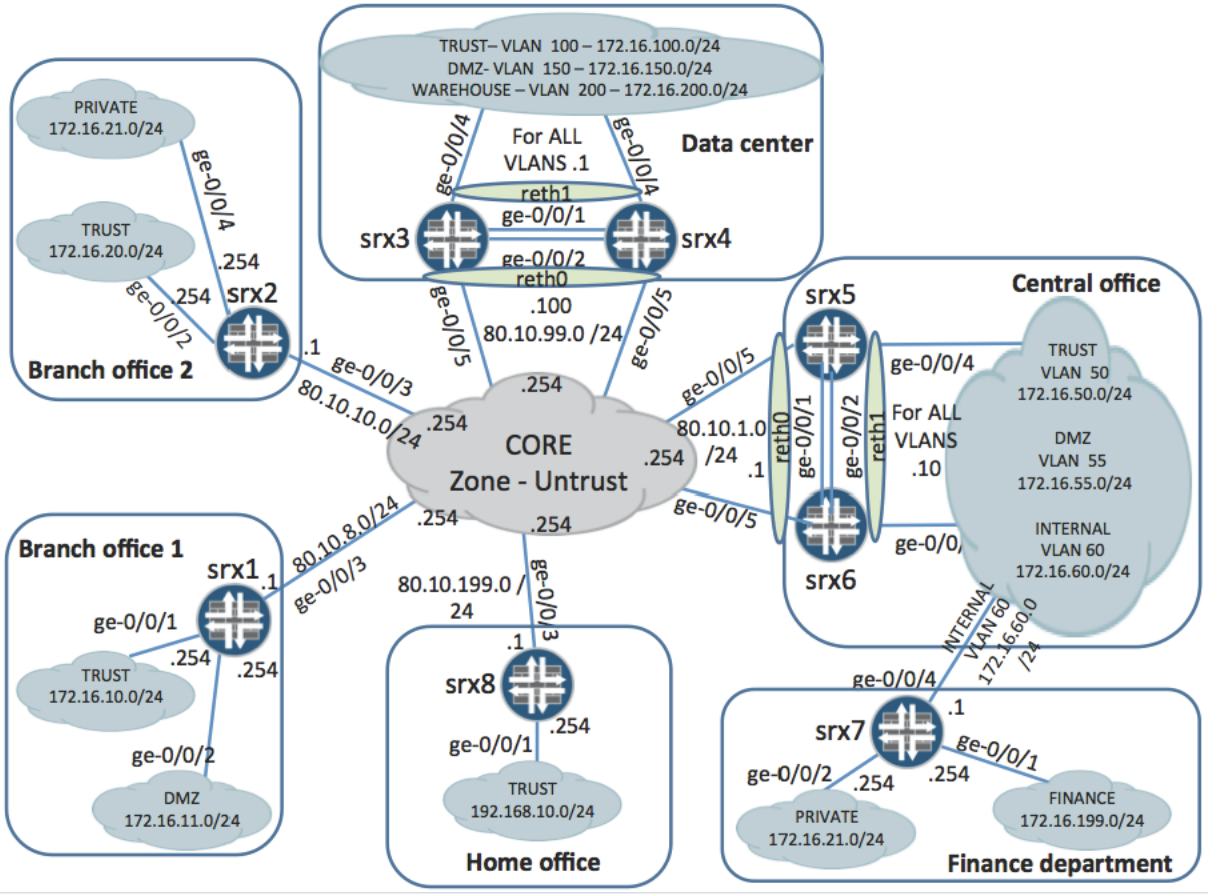
NOTE: The following step is **informational** as the redundancy group IP address monitoring functionality is available only on High end SRX devices!

    g. In addition configure IP monitoring/tracking for every created redundancy group with following aspects:
        i. Track:
            1. gateway (next-hop) to the CORE network.
            2. IP address of srx7's interface from the INTERNAL zone
        ii. Use appropriate (nearest, not requiring specific security policy) reth interface for tracking.
        iii. The secondary node, e.g. the node having the backup interfaces, should also monitor all these IPs by using different source IP addresses. These IP addresses are incremented IP addresses (by one) of the selected reths.
        iv. Only failure of all tracked IP addresses will trigger redundancy group failover
        v. Failure is represented by 4 successive failed probes/pings and the detection has do be done in 8 seconds.

Chapter three: Firewall - Security policies

This chapter deals with the security policies on the SRX devices. You will configure security policies on the SRX devices to satisfy requirements given in the individual tasks. Within this chapter you will also configure the interfaces, IP addresses and security zones.

Topology for chapter three:



You can continue with the configuration in case you have completed tasks from the previous chapter. OR load the latest initial configurations for this chapter to the devices.

NOTE: In case you have already loaded the initial configuration for the switches (vr-device and access switch) before you don't have to do it again.

NOTE: The labs starting point requires to have SRX clusters formed between devices srx3 srx4 and srx5 srx6 and the respective configuration loaded on them.

TIP: Ensure you read this entire chapter, before starting with the first task.

Task 1: Configuring interfaces and security zones

In this part you will configure the interfaces, zones and assign interfaces to zones.

1) Configure the interfaces on every device according to the table below. The table reflects the topology image.
The association of loopback interfaces to zones is up to your selection unless explicitly defined by a given task.

Device	Interface	IP address	VLAN-ID	Zone
srx1	ge-0/0/1.0	172.16.10.254/24	None	TRUST
srx1	ge-0/0/2.0	172.16.11.254/24	None	DMZ
srx1	ge-0/0/3.0	80.10.8.1/24	None	UNTRUST
srx2	ge-0/0/2.0	172.16.20.254/24	None	TRUST
srx2	ge-0/0/3.0	80.10.10.1/24	None	UNTRUST
srx2	ge-0/0/4.0	172.16.21.254/24	None	PRIVATE
Cluster1 (srx3, srx4)	reth0	80.10.99.100/24	None	UNTRUST
Cluster1 (srx3, srx4)	reth1.100	172.16.100.1/24	100	TRUST
Cluster1 (srx3, srx4)	reth1.150	172.16.150.1/24	150	DMZ
Cluster1 (srx3, srx4)	reth1.200	172.16.200.1/24	200	WAREHOUSE
Cluster2 (srx5, srx6)	reth0	80.10.1.1/24	None	UNTRUST
Cluster2 (srx5, srx6)	reth1.50	172.16.50.10/24	50	TRUST
Cluster2 (srx5, srx6)	reth1.55	172.16.55.10/24	55	DMZ
Cluster2 (srx5, srx6)	reth1.60	172.16.60.10/24	60	INTERNAL
srx7	ge-0/0/1.0	172.16.199.254/24	None	FINANCE
srx7	ge-0/0/2.0	172.16.21.254/24	None	PRIVATE
srx7	ge-0/0/4.60	172.16.60.1/24	60	INTERNAL
srx8	ge-0/0/1.0	192.168.10.254/24	None	TRUST
srx8	ge-0/0/3.0	80.10.199.1/24	None	UNTRUST

Task 2: Local traffic and static routing

This part is focused on handling the traffic destined for the devices themselves.

1) Allow ping on all configured interfaces.
2) Allow ospf protocol communication on all interfaces connected to the CORE.
3) Allow ssh connections to all interfaces associated with the TRUST zone on every device.
4) Ensure the management interfaces allow following services: ssh, telnet, http, https, snmp and ntp. In addition ensure the srx8 allows for SNMP queries from 2.2.2.0/28 network.
5) Create static default route on each device pointing to the CORE network.
6) Configure the necessary routes using static configuration to provide connectivity for the PRIVATE zone in the Finance department through the cluster 2.
7) Create static route for accessing the NTP, SYSLOG, SNMP servers using the management network. The management network range is 10/8 and the next-hop for the srx devices is 10.10.1.254.

Task 3: Security policies

Here you will configure security policies to enforce listed restrictions on the transit traffic.

Below are details about networks which are referenced in the tasks:

Name	Network range
Private corporate network	172.16.0.0/16
Internet	0.0.0.0/0

Branch office 1: srx1

1) The hosts from the TRUST zone and its network range can go to the outside network (internet) with http and https.
2) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.
3) Devices in the DMZ zone should be accessible from the whole private corporate network including the local TRUST zone with https.
4) No other connections are allowed to go in or out of the TRUST zone.
5) No connections are allowed to go out from DMZ zone. Log all violations going out to the CORE network.

Branch office 2: srx2

6) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.
7) No other connections are allowed in or out of the TRUST zone. Log all outgoing violations to the destinations reachable via the CORE network.
8) Hosts from the PRIVATE zone can connect to the DMZ zone in the Central office and Data center using ssh, http, https, ftp, telnet.

Home office: srx8

9) Hosts connected to the srx8 can access the whole private corporate network regardless of the application and in addition have http and https permitted to the outside world/internet.

Finance department: srx7

10) From the FINANCE zone all connections are allowed to the INTERNAL zone and to the WAREHOUSE zone in the Data center only for SQL queries. The database server in Data center listens on ports 5000 6000. Ensure the appropriate ALG for SQL is being used.
11) DMZ zones in the Data center and Central office are reachable from the FINANCE zone using http, https and ssh.

Data center: cluster1

12) The TRUST zone has access to the whole private corporate network (also locally connected networks) with any application.
13) No other connections are allowed in or out of the TRUST zone. Log all outgoing violations,e.g. connections going to CORE network.
14) Full communication between DMZ (local and central office) and WAREHOUSE zone is possible in both directions.
15) Http, https, ssh, smtp, ftp and telnet connections from the private corporate network (reachable via CORE network) to DMZ are allowed.
16) Only the specific SQL connections (described previously) from the FINANCE zone in the Finance department are allowed to enter the WAREHOUSE zone. Count this traffic.

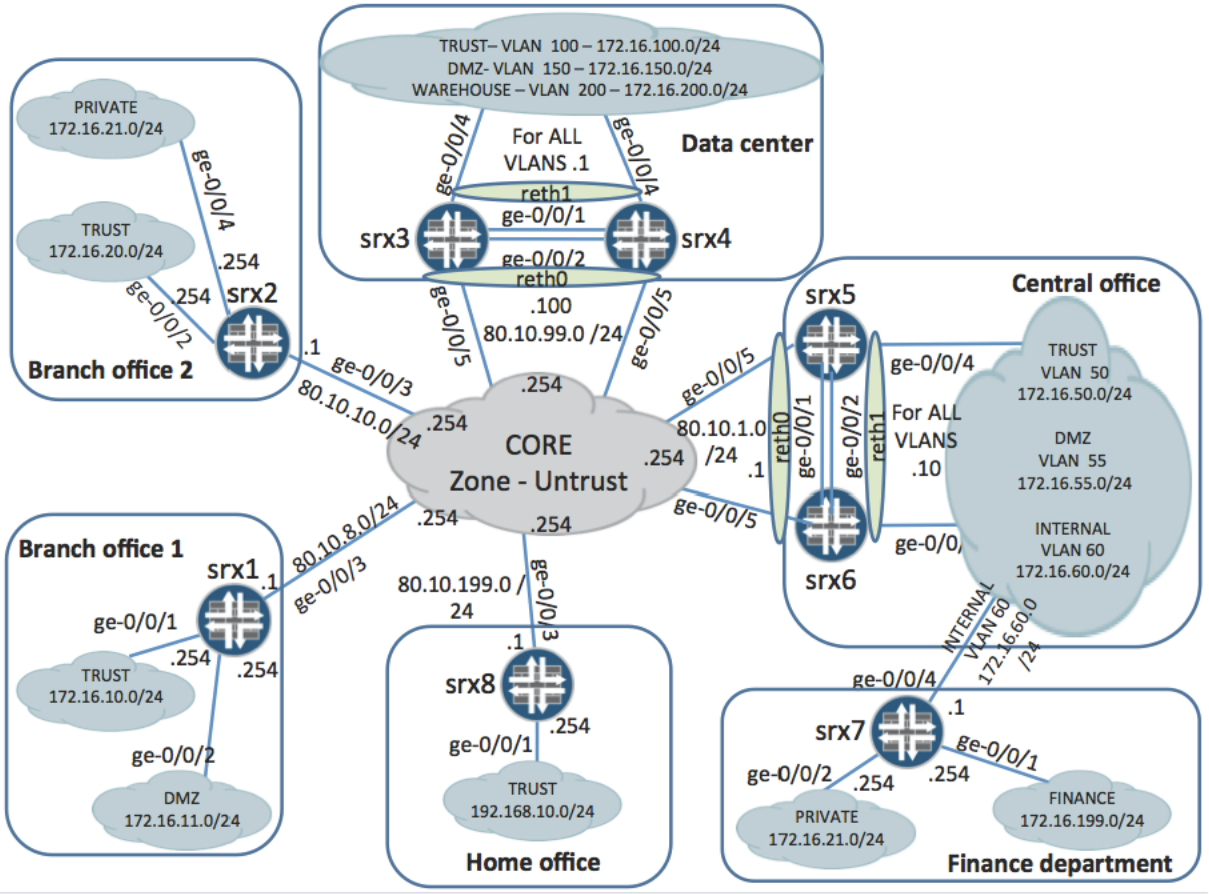
Central office: cluster2

17) Ensure the permitted connections from the Finance department on the srx7 are allowed as well, but focus only network ranges and not applications, i.e. when defining these policies disregard the applications.
18) Hosts located in the INTERNAL zone have full access to the local DMZ resources but only during working days and working hours (8:00 - 18:00).
19) The TRUST zone has access to the whole private corporate network (also locally connected networks) with any application. In addition only http and https access is allowed to the internet from the TRUST zone. Log all outgoing violations.
20) Full communication between DMZ and WAREHOUSE zone is possible in both directions.
21) Http, ftp and telnet requests sourced from the private corporate network arriving on the core network facing interface and destined to the DMZ hosts need to be authenticated in order to be granted. Use the pass-through authentication with following settings
    a. username: testuser, password: testuserpw123
    b. 1 hour of inactivity will result in re-authentication
    c. the password are stored locally on the security device
    d. ftp and telnet banners:
        i. initial banner: “Look out firewall authentication!!!”
        ii. in case of successful authentication: “Correct!”
        iii. in case of unsuccessful authentication: “Incorrect!”
22) SSH and HTTPS connections from private corporate network arriving on the core network facing interface and destined to the DMZ hosts the are granted without authentication.
23) Ensure DNS information is not changed when using NAT and ensure that the domain-name length for DNS packets is validated

Chapter four: Unified Threat Management

This chapter is dedicated to the Unified Threat Management (UTM) functionality on Junos security devices. The presented tasks will require you to configure web-filtering, content filtering, antivirus and anti-spam features.

Topology for chapter four:



You can continue with the configuration in case you have completed tasks from the previous chapter. Or load the latest initial configurations for this chapter to the devices.

NOTE: The labs starting point requires to have SRX clusters formed between devices srx3 srx4 and srx5 srx6 and the respective configuration loaded on them.

NOTE: In case you have loaded the initial configuration for the switches (not shown in the topology) before you don't have to do it again.

TIP: Ensure you read this entire chapter, before starting with the first task.

Task 1: Web-filtering

In this section you will configure the web-filtering on the security devices in branch office, central office and home office.

Try to use existing security policies whenever possible.

Branch office: srx1

1) Protect the http traffic from the TRUST zone to the UNTRUST zone by enabling web-filtering which fulfills following requirements.
2) The integrated Surf-control type of web-filtering should be used.
3) The device handles the returned categories in following way:
    a. Hacking, Violence, Gambling, Games --> block these categories
    b. News, Computing_Internet --> permit these categories
    c. All other URLs --> permit but log the requests
4) In case of blocked site the clients should receive following message: "Blocked site!"
5) In case the engine has difficulties due various reasons the traffic handling should be:
    a. In case the engine experiences too many requests the subsequent requests are blocked
    b. When problems with server communication (such as reaching the timeout for receiving the responses or server connectivity loss) occur the requests are blocked
    c. For all other causes the requests are permitted but logged
6) The timeout for the server responses is 120 seconds.
7) The results from SurfControl server should be locally cached for 30 minutes and the amount of cached data should not exceed 1 MB (1024 KB, 1048576 B).
8) The SurfControl server is reachable at 85.115.54.170 port 62252.

Central office: cluster 2

9) The web-filtering in the central office uses other method as the device in the Branch office, namely the WebSense option.
10) The protection happens from the TRUST zone to the UNTRUST zone.
11) The following URLs are excluded from the checking on the WebSense server and are permitted right away (http pages are assumed here):
    a. Sites ending with "bing.com" are permitted
    b. The same applies for google.com sites
    c. The www.juniper.net site is allowed
12) The following URLs should be instantly denied regardless of the WebSense handling:
    a. www.facebook.com
13) The WebSense server is located at 80.200.200.200 and the communication port is 12345.
14) In case the security device has communication issues with the WebSense server it should block the requests. If other problems are experienced by the engine the requests are permitted but need to be logged, this includes the too many requests situation.
15) Set the communication timeout with the WebSense server to 180 seconds.

16) The client's notification about dropped requests has to be this custom message: "SRX blocked the request!"
17) The requests forwarded from security device in the central office need to carry information about redirect account to achieve specific treatment and rule enforcement at the WebSense server. The redirect account value is "centraloffice".
18) The number of connections to the WebSense server has to be below 6.

Home office: srx8

19) The srx8 device should enforce the web filtering on the traffic from TRUST zone to the UNTRUST zone.
20) The web-filtering decisions are done entirely by the security device itself without any remote server interactions.
21) The following URLs are denied:
    a. www.facebook.com
    b. www.myspace.com
22) All other URLs are permitted.
23) If a request is blocked the clients will receive following message: "This page is not allowed!"
24) All issues or problems with processing the requests result in blocking behaviour.

Task 2: Antivirus

This part contains the tasks related to the antivirus feature that need to take place on the srx8 device.

Home office: srx8

1) The antivirus protection needs operate in comprehensive protection mode, e.g. full file-based scanning utilizing the full database and being capable of applying heuristics methods.
2) Checks for database updates every 2 hours are automatically performed by the device.
3) The antivirus scanning has to be done on http, ftp and smtp traffic going from the TRUST zone to the internet (UNTRUST zone). Use the existing policy, if needed modify it.
4) Exclude the www.company.com traffic from being scanned.
5) Exclude the video, application and audio mime types from being scanned including their subtypes with the exception of application/javascript and application/ecmascript, e.g. application/javascript and application/ecmascript are subject to antivirus scan.
6) Ensure the compressed files are scanned up to the 2 ^{d} level of compression.
7) Antivirus scanning has to be performed on all files regardless of their extension.
8) Enable intelligent prescreening.
9) Set the scan engine timeout to 10 minutes.
10) If the antivirus engine detects a virus, the infected message has to be changed by deleting the original content and the notification "AV Engine detected virus!" needs to be included. In case the virus was found in an email message, the sender needs to receive a message having subject "AntiVirus" and body "AV Engine detected virus!".
11) All fallback options are set to block except the default action which permits the traffic and generates a log about it.
12) Fallback notifications generation is according to the requirements below:
    a. Action BLOCK
        i. for non-email protocols message "AV denied the message, because it was not able to scan it!" will be sent to the application (e.g. application/protocol error will be generated)
        ii. for email protocols an email is sent to sender with subject "AntiVirus" and body"AV denied the message, because it was not able to scan it!"
    b. Action NON-BLOCK
        i. for email protocols the engine sends the message to the recipient, but tags the subject with "AntiVirus" and body"AV was not able to scan the message!"
13) In case the AV needs longer time for examination, it should send every 25 seconds unchecked small parts of the file to the receiver side to prevent timeout from occurring.

Task 3: Content filtering

This part lists the requirements for the content filtering performed on the central office security device.

Central office: cluster 2

1) The content filter has to be enforced on the http traffic from TRUST zone to the UNTRUST zone.
2) Ensure the device blocks:
    a. http content types: exe files, cookies and java applets
    b. mime: all video types
    c. files with the extensions bat and sh
    d. http protocol command TRACE
3) The device should generate protocol errors when blocking with custom message: "Blocked content by SRX!"
4) Limit the number of sessions per client to 15, the connections above are blocked.

Task 4: Antispam

The requirements for the antispam feature are listed here.

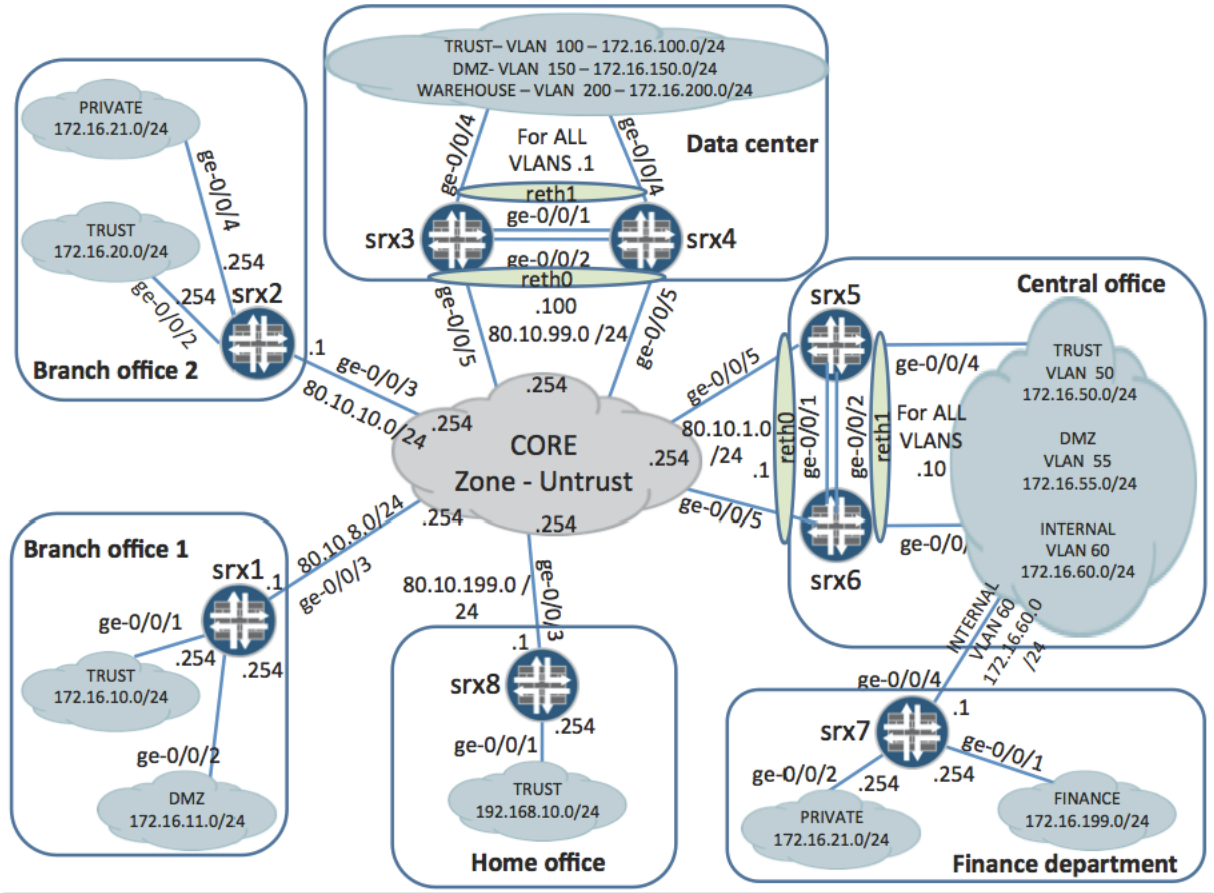
Central office: cluster 2

1) One of the company email servers is located in the DMZ zone in the central office. The email server IP address is 172.16.55.100.
2) The SMTP communication from the outside world going to this email server needs to be inspected. If needed create appropriate security policy for this purpose (in the correct context of security zones, using correct address books and application).
3) The SMTP messages received from the 5.5.5.4 address are considered malicious but from the 5.5.5.5 IP address are valid and allowed. The 123.123.123.123 host is considered potentially dangerous too. The company internal policy defines to tag the subject in these email messages with the prefix "SPAM!!!".
4) Similarly the domains and email addresses below are considered potentially dangerous and therefore marked accordingly, e.g. tagging the email subject as in the previous case.
    a. Domains: bad.com, spam.com
    b. Email addresses: spam@company.com, adv@company.com
5) The security device performs the decisions internally without consulting any external resources, e.g. external SBLs are not used.

Chapter five: IPSec VPNs

This chapter is concentrated on IPSec VPN implementations. You will configure Policy-based IPSec VPN, Route-based IPSec VPN with OSPF, GRE tunnel over Route-based IPSec VPN with OSPF and Dynamic VPN.

Topology for chapter five:



You can continue with the configuration in case you have completed tasks from the chapter 3.

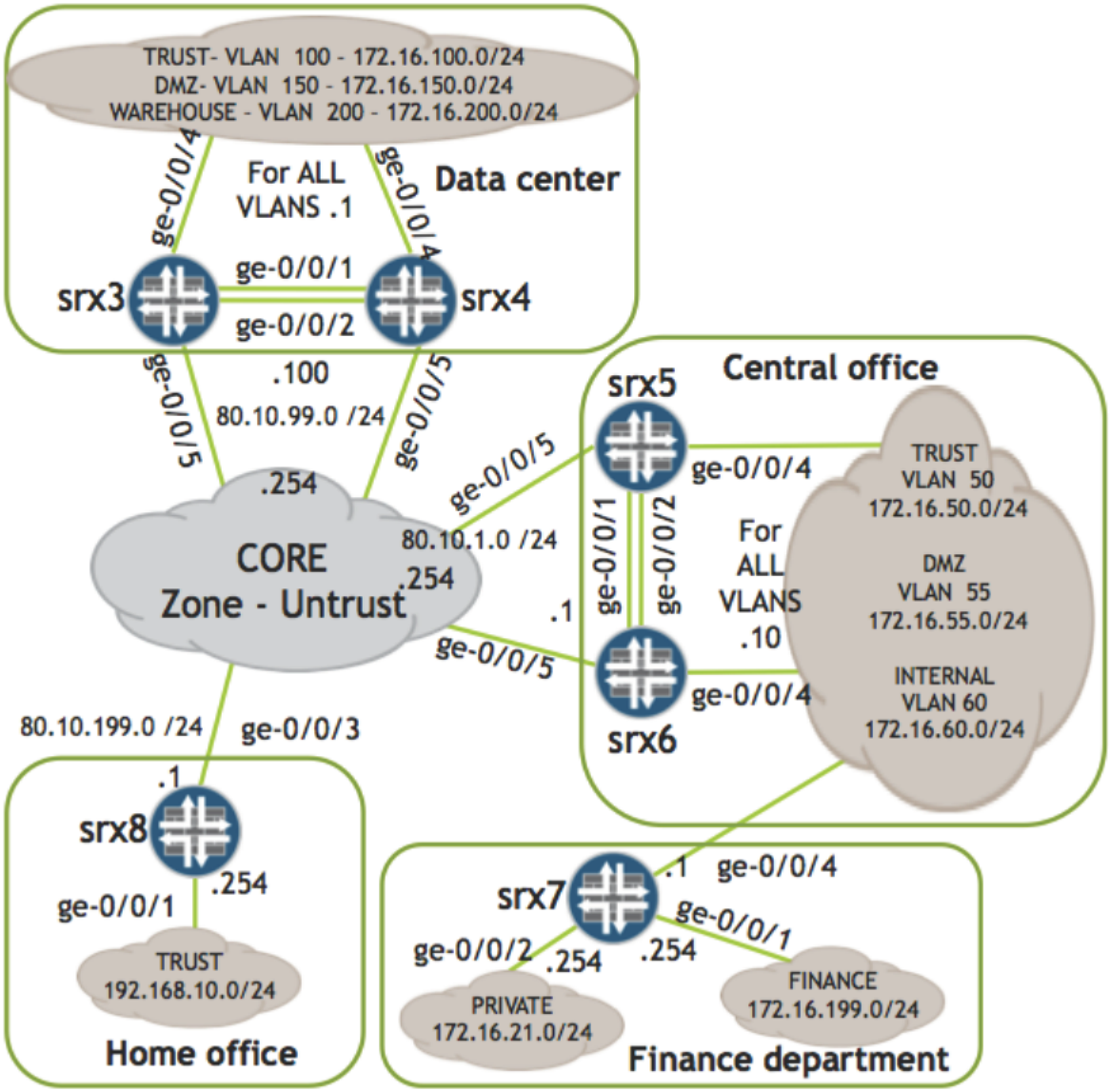
NOTE: The labs starting point requires to have SRX clusters formed between devices srx3 srx4 and srx5 srx6 and the respective configuration loaded on them.

NOTE: In case you have loaded the initial configuration for the switches (not shown in the topology) before you don't have to do it again.

TIP: Ensure you read this entire chapter, before starting with the first task.

Task 1: Configuring Policy-based VPN

Task 1 Topology.



In this part you will configure the lab equipment as necessary to build Policy-based VPN between the Data Center, Home Office and Finance department.

1) Configure the IPSec VPN on every device according to the table below, which reflects the topology image.

Local Peer	Interface	Security zone	Remote Peer	Interface	Security zone
srx7	ge-0/0/4.60	Untrust	Cluster1	reth0.0	Untrust
srx8	ge-0/0/3.0	Untrust	Cluster1	reth0.0	Untrust

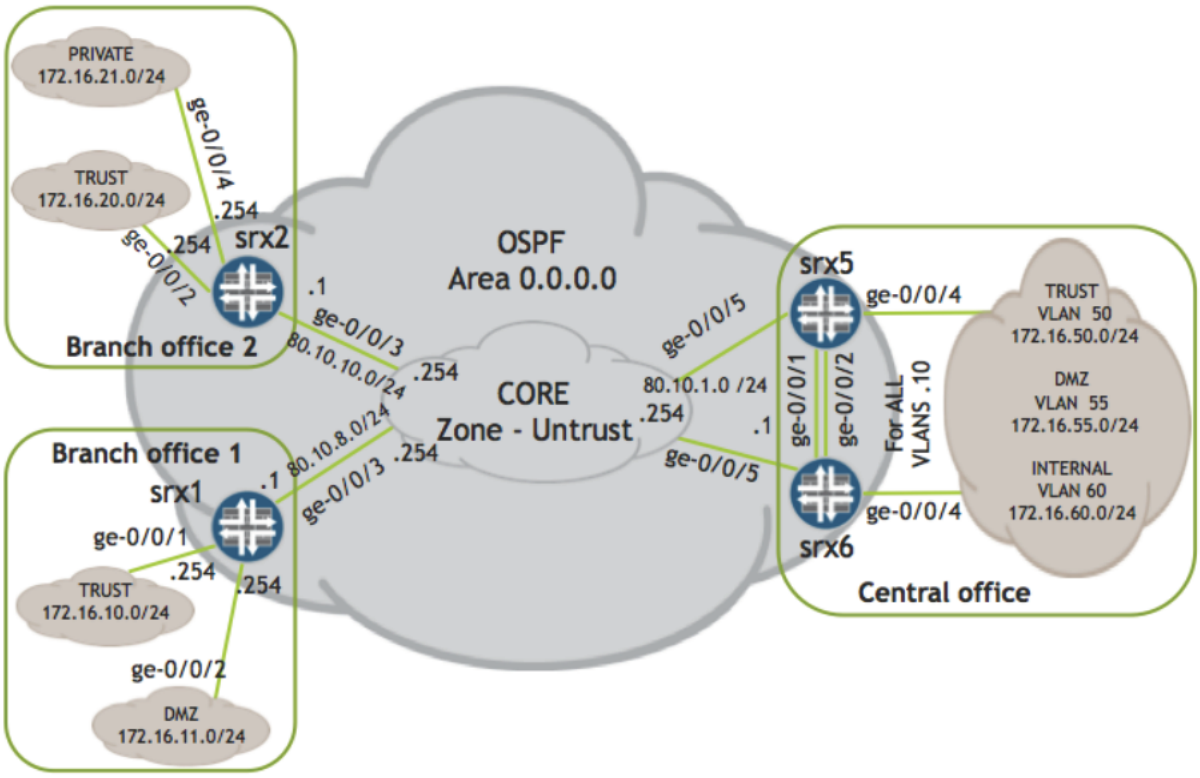
2) Central Office srx5/srx6 cluster provides only dynamical NAT-SRC service.
3) The VPN between srx8 and Cluster1 must meet following requirements:

a. Validate peer reachability with DPD option. The keepalives should be sent to the neighboring peer regardless of traffic patterns every 10 seconds. Consider the peer unreachable if the number of DPD retransmissions exceeds 5 packets.
b. IKE phase 1 proposal must include: preshared key “juniper”, DES, DH G1, MD5. Rekey Phase1 every 24 hours.
c. IKE phase 2 proposal must include: AES128, ESP, DH G2, SHA1. Rekey Phase2 every 12 hours.
d. Ensure that any traffic originated from the Trust zone of the Home Office can only reach the TRUST zone located in the Data Center and vice versa.
e. Collect the IKE Phase2 security association’s management events in the kmd file on cluster1.

4) The VPN between srx7 and Cluster1 must meet following requirements:
   a. Validate peer reachability with DPD option. The keepalives should be sent to the neighboring peer regardless of traffic patterns every 10 seconds. Consider the peer unreachable if the number of DPD retransmissions exceeds 5 packets.
   b. IKE phase 1 proposal must include: preshared key “inetzero”, 3DES, DH G5, SHA1. Rekey Phase1 every 24 hours.
   c. IKE phase 2 proposal must include: AES192, ESP, SHA1. Rekey IPSec tunnel on transmitting 5 MB of traffic.
   d. Ensure that only traffic originated from the FINANCE zone of srx7 can reach the Warehouse zone located in the Data Center and vice versa. This traffic must trigger tunnel establishment.
   e. Collect the IKE Phase2 security association’s management events in the kmd file on the cluster1.

Task 2: Configuring Route-based VPN

Task 2 Topology.



In this part you will configure lab equipment as necessary to build full meshed Route-based VPN between Central Office, Branch office 1 and Branch office 2.

1) Branch offices have direct tunnel to each other and can communicate either directly or via the Data Center. The forwarding decision is done on the base of tunnel's state.
Configure the interfaces on every device according to the table below, which reflects the topology image.

Device	Interface	IP address	VLAN-ID	Zone
srx1	st0.0	11.0.0.2/30	None	Untrust
srx1	st0.1	11.0.0.10/30	None	Untrust
srx2	st0.0	11.0.0.6/30	None	Untrust
srx2	st0.1	11.0.0.9/30	None	Untrust
Cluster2 (srx5, srx6)	st0.0	11.0.0.1/30	None	Untrust
Cluster2 (srx5, srx6)	st0.1	11.0.0.5/30	None	Untrust

Configure the IPSec VPN on every device according to the table below, which reflects the topology image.

Local Peer	Interface	Remote Peer	Interface
Cluster2	reth0.0	srx1	ge-0/0/3.0
Cluster2	reth0.0	srx2	ge-0/0/3.0
srx1	ge-0/0/3.0	srx2	ge-0/0/3.0

2) In this task's topology you will use OSPFv2 as the IGP routing protocol.
The subnets located in the TRUST, PRIVATE, INTERNAL or DMZ zones must appear as OSPF internal routes on all devices in OSPF area 0, but no IGP adjacencies may be formed across interfaces located within these security zones. Ensure that traffic originated from any TRUST zone can reach any destination in the TRUST zone.

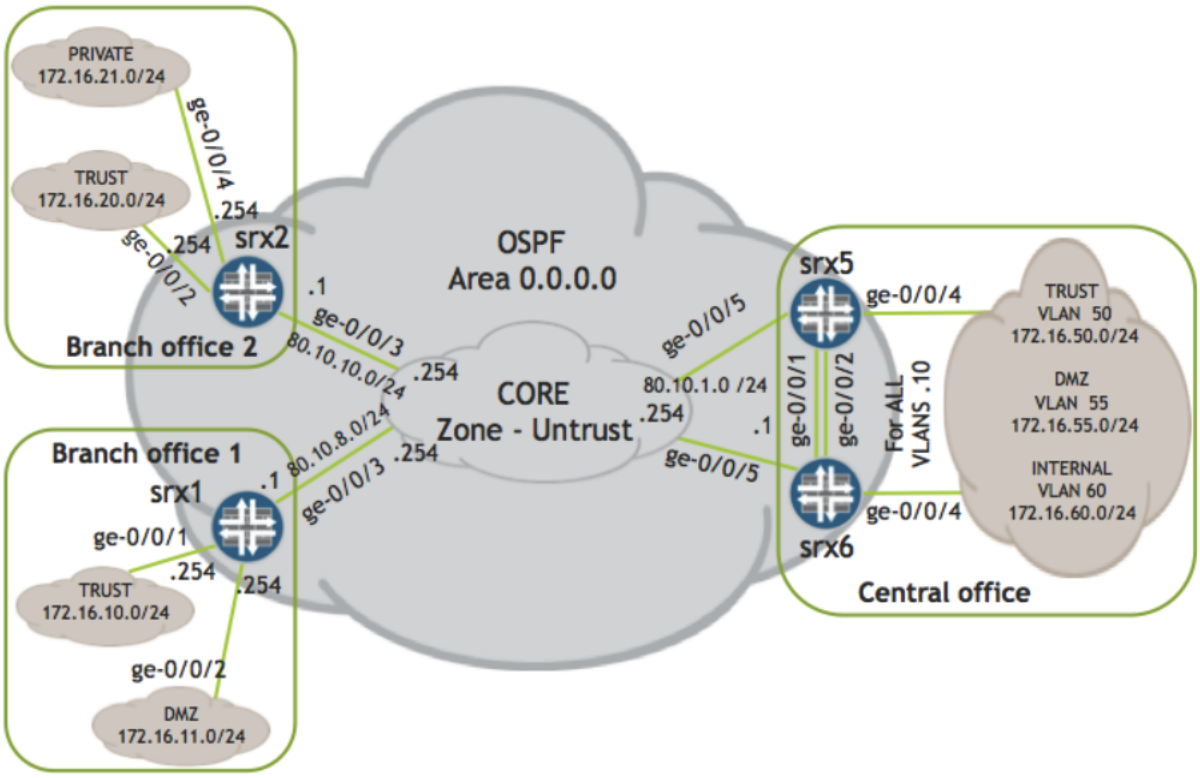
Configure the interfaces on every device according to the table below.

Device	Interface	OSPF Area
srx1	st0.0	OSPF Area 0
srx1	st0.1	OSPF Area 0
srx1	ge-0/0/1.0	OSPF Area 0
srx1	ge-0/0/2.0	OSPF Area 0
srx2	st0.0	OSPF Area 0
srx2	st0.1	OSPF Area 0
srx2	ge-0/0/2.0	OSPF Area 0
srx2	ge-0/0/4.0	OSPF Area 0
Cluster2 (srx5, srx6)	st0.0	OSPF Area 0
Cluster2 (srx5, srx6)	st0.1	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.50	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.55	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.60	OSPF Area 0

3) The VPN between srx1 and Cluster2 and between srx2 and Cluster2 must meet the following requirements:
   a. Rekey IPSec tunnel every 8 hours;
   b. Validate data path with VPN monitor option. The keepalives should be sent to the neighboring peer regardless of traffic patterns with 5 sec interval. It is allowed to miss only three consecutive keepalives after which the tunnel is considered inactive.
   c. IKE phase 1 proposal must include: preshared key "inetzero", AES128, DH G2, SHA.
   d. IKE phase 2 proposal must include: AES256, ESP, SHA1.
   e. Ensure that in case of one tunnel's failure traffic originated from the TRUST security zone of any site still can reach other site's protected resources.
4) The VPN between srx1 and srx2 must meet the following requirements:
   f. Rekey IPSec tunnel on transmitting 100 MB of traffic;
   g. Validate data path with VPN monitor option. The keeplives should be sent to the neighboring peer only in absence of traffic patterns.
   h. IKE phase 1 proposal must include: preshared key "inetzero", 3DES, DH G2, MD5.
   i. IKE phase 2 proposal must include: AES256, ESP, SHA1.
   j. Ensure that in case of one tunnel's failure traffic originated from the TRUST security zone of any site still can reach other site's protected resources.

Task 3: Configuring GRE-tunnel over Route-based VPN

Task 3 Topology.



In this part you will configure the lab equipment as necessary to build GRE-tunnel over Route-based VPN between Branch Office 1 and Branch Office 2.

1) Configure the interfaces on every device according to the table below.
The GRE tunnel source should be configured as device's local lo0 interface address and the destination should be configured as remote device's lo0 interface address.

Device	Interface	IP address	VLAN-ID	Zone
srx1	gr-0/0/0.0	11.11.11.1/30	None	Untrust
srx1	lo0.0	192.168.1.1/32	None	Untrust
srx2	gr-0/0/0.0	11.11.11.2/30	None	Untrust
srx2	lo0.0	192.168.1.2/32	None	Untrust

2) You need to configure OSPFv2 as the IGP between Branch Office 1 and Branch Office 2. Configure the interfaces on every device according to the table below, which reflects the topology image.

Device	Interface	OSPF Area
srx1	gr-0/0/0.0	OSPF Area 0
srx2	gr-0/0/0.0	OSPF Area 0

3) Ensure that any traffic originated from the TRUST zone of Branch Office 1 can reach the TRUST zone of the Branch Office 2 vice versa.

Task 4: Configuring Dynamic VPN

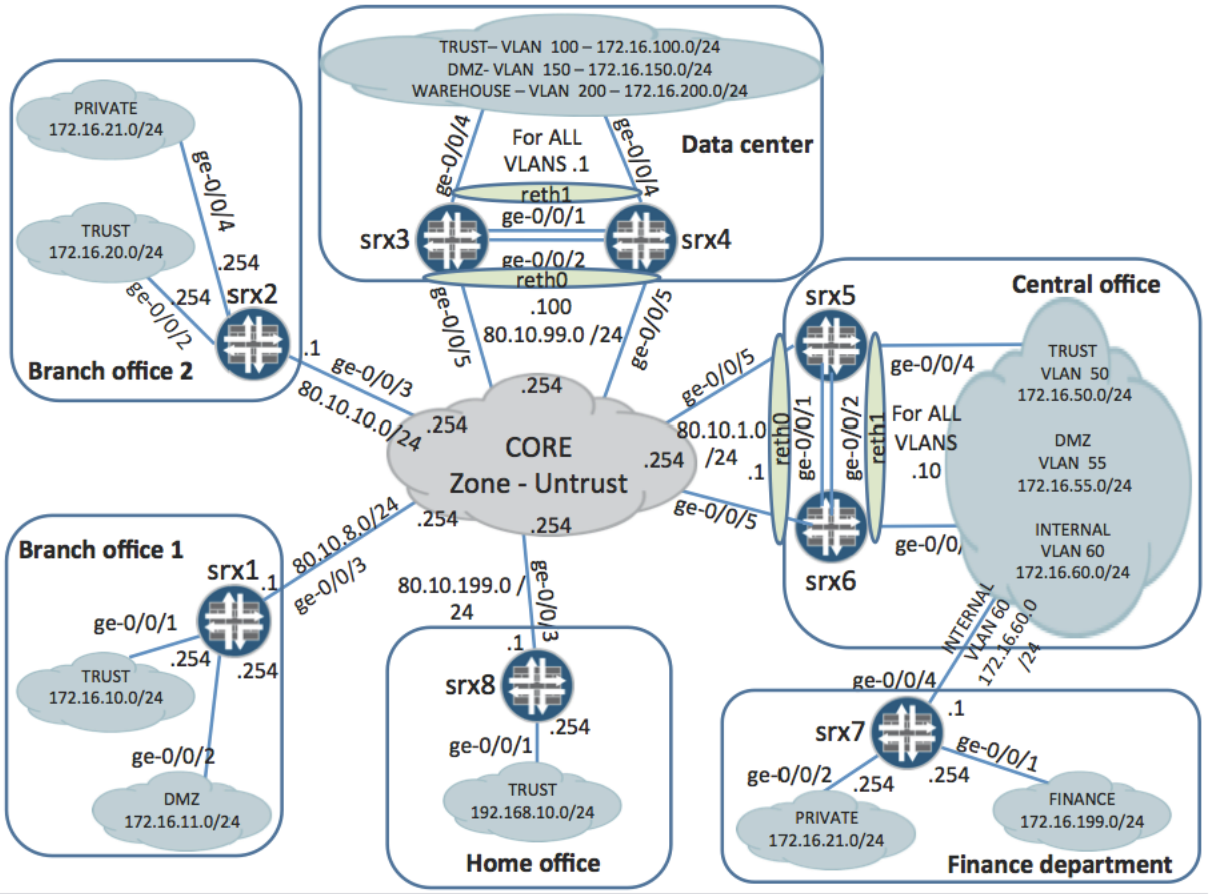
In this part you need to configure remote access to the Data Center's protected resources located in the WAREHOUSE security zone. Configure remote access via IPSec VPN for the client's machine located in the CORE network in such way that it satisfy following requirements.

1) The initial client's connection can be established only via https on the IP address 80.10.99.100.
2) User must be authenticated with following settings:
    a. username: testuser, password: testuserpw123
    b. reauthentication after 1 hour of inactivity
    c. local authentication
    d. banners:
        iv. in case of successful authentication: "Correct!"
3) Use predefined proposals "Basic" for IKE Phase1 and Phase2.
4) The IP address allocated to client's IPSec tunnel must be borrowed from the range of IP addresses 172.16.200.150 172.16.200.159.
5) Ensure that client has access to the Data Center network 172.20.100.0/24 via the IPSec tunnel. The traffic destine to other prefixes must bypass IPSec tunnel.

Chapter six: NAT

This chapter is focused on different NAT implementations. You will configure source NAT, destination NAT and static NAT.

Topology for chapter six:



You can continue with the configuration in case you have completed tasks from the chapter 3. Or you can load the latest initial configurations for this chapter to the devices.

NOTE: The labs starting point requires to have SRX clusters formed between devices srx3 srx4 and srx5 srx6 and the respective configuration loaded on them.

NOTE: In case you have loaded the initial configuration for the vr-device and the access-switch before you don't have to do it again.

TIP: Ensure you read this entire chapter, before starting with the first task.

Task 1: IPv4 Source NAT

In this part you will configure source NAT on srx1, srx2 and srx8 as necessary to enforce listed scenarios between private and public IP addresses.

Home office: srx8

1) The hosts located in Home Office are using IP addresses from the subnet 192.168.10.0/24, which is a non-routable prefix in the Core network.
   Configure srx8 that any host located in the TRUST zone in the Home office can reach all IP routable prefixes in the Core network.
2) Ensure IP addresses and ports translation mappings are maintained for 1 hour after the sessions are closed. The external hosts can reach the internal hosts by using their reflexive IP address only when they previously have received packet(s) from the internal host.

Branch office 1: srx1

3) Configure srx1 to apply NAT to all sessions originated in the network 172.16.10.0/24 and destined to any routable prefixes in the Core network. Also to all sessions originated in the network 172.16.11.0/24 and destined to prefixes associated with Data Center and Central office core facing subnets.
4) For sessions originating in the network 172.16.10.0/24 ensure that:
   a. The public range 80.10.8.16/28 is used for address translation if a session is going from TRUST to UNTRUST zone. PAT is not allowed;
   b. If pool of IP addresses is exhausted the egress interface's IP address must be used for translation;
   c. Private IP addresses 172.16.11.201 172.16.11.206 are used for address translation if session goes from TRUST to DMZ zone. PAT is allowed;
5) For sessions originated in the network 172.16.11.0/24 ensure that:
   a. The public range 80.10.8.64/27 is used for address translation if a session goes from DMZ to UNTRUST zone. PAT is allowed;
   d. Private IP addresses 172.16.10.97 172.16.10.110 are used for address translation if session originates in the DMZ and goes to the TRUST zone. PAT is not allowed;
   e. If the pool of IP addresses is exhausted the egress interface's IP address must be used for translation;
   f. Ensure that multiple concurrent sessions from the same host always use the same IP address.

Branch Office 2: srx2

6) On srx2 the source NAT should be applied to sessions originated either in the PRIVATE or TRUST zones having the source IP addresses from ranges of 172.16.21.16 172.16.21.71 and 172.16.20.200 - 172.16.20.209 and are destined to any addresses from the 80.10.0.0/16 address range. For translation use the IP addresses from the subnet 80.10.10.128/25;
7) Ensure the same internal host from one of the ranges above always uses the same public IP address for outgoing sessions;
8) Ensure that all remaining connections will always be translated to the IP address of the egress interface.

Task 2: IPv4 Destination NAT

In this part you will configure cluster1 as necessary to provide access to resources located in the TRUST, DMZ and WAREHOUSE zones in the Data Center.

Data center: cluster 1

1) There are two public addresses used to provide access to the protected resources in the Data Center network 80.10.99.101 and 80.10.99.102;
2) The IP address 80.10.99.101 should be mapped to the IP address 172.16.100.1 located in the TRUST zone. PAT is not allowed. Ensure that only sessions initiated from IP addresses associated with Branch and Home Offices 1 and 2 are translated by NAT;
3) The IP address 80.10.99.102 should be mapped to the IP addresses in the DMZ, TRUST and WAREHOUSE zones based on conditions defined in the table below:

Public IP address	Public port number	Private IP address	Private port number
80.10.99.102	21	172.16.100.1	21
80.10.99.102	23	172.16.150.1	23
80.10.99.102	8080	172.16.200.1	80

4) Ensure that all not translated IP packets destined to the 80.10.99.101 and 80.10.99.102 IP addresses are dropped;
5) Ensure that all packets destined to the TRUST zone's resources look as they are originated from the cluster1 itself.

Task 3: IPv4 Static NAT

This section is dedicated to static NAT configuration. You need to configure cluster2 and srx7 to allow bidirectional NAT translations for some of the protected resources located in the following sites.

Central office: cluster 2

1) Using the cluster 2 ensure the rest of the enterprise network (connecting through the Core network) sees the srx7 loopback address as 80.10.1.11. Srx7 must be able to initiate and accept sessions to/from other security devices in the Core network.
2) The range of IP addresses 80.10.1.128/29 must be mapped to the similar range of IP addresses in the DMZ zone, e.g. to 172.16.55.128/29.

Finance department: srx7

3) On srx7 the 172.16.21.0/26 subnet from the PRIVATE zone and the 172.16.199.0/26 subnet from the FINANCE zone should be hidden from the rest of the corporate network. For access to and from these networks the IP addresses from the range 172.16.60.128/25 have to be used. The mapping should employ shifting and start at 172.16.60.128 <--> 172.16.21.0.
4) Ensure that all IP packets with untranslated destination IP addresses will be dropped.

Task 4: NAT Protocol Translation (IPv6/IPv4)

This section focuses on enabling IPv6 and IPv4 hosts to communicate with each other by using NAT.

Branch 2

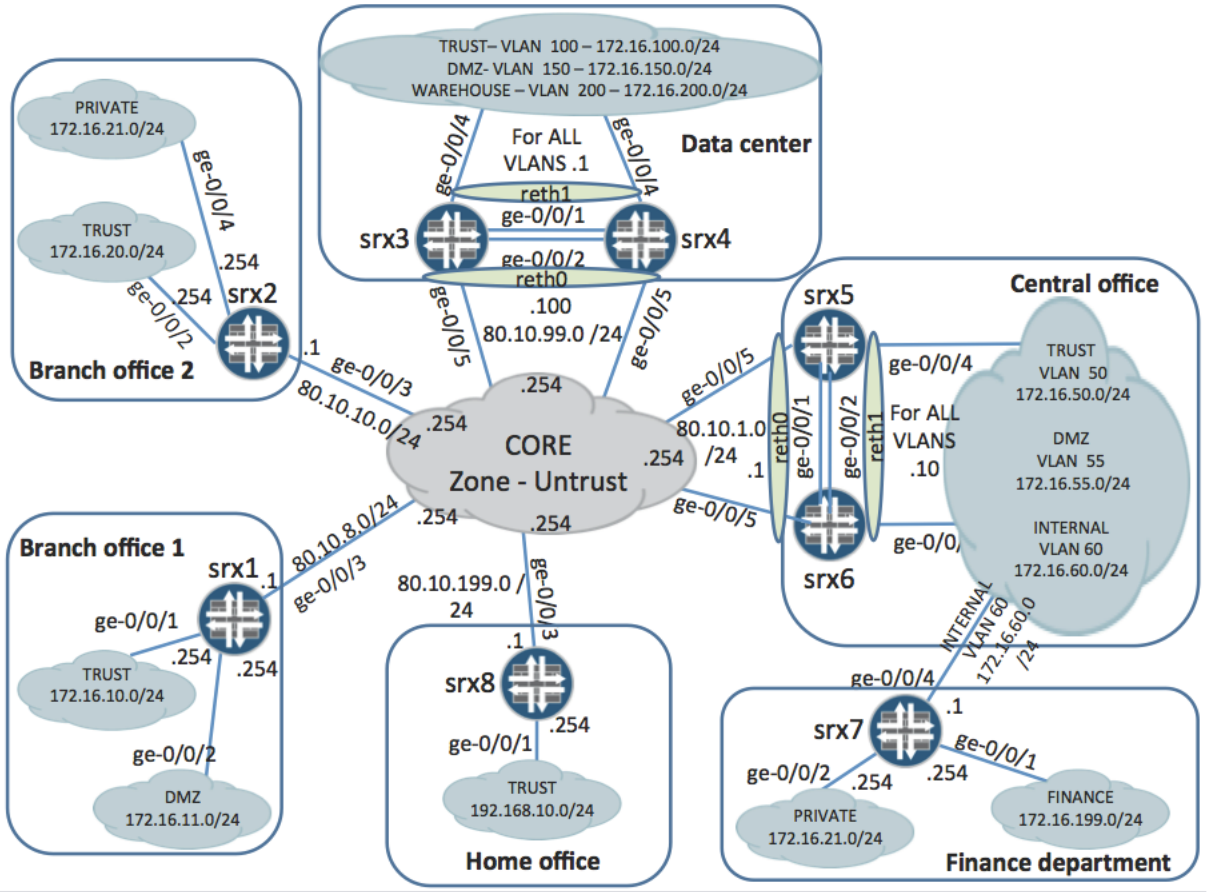
1) Ensure that IPv6 users attached to the PRIVATE zone in Branch2 can reach the IPv4 host 80.10.10.100 by sending and receiving traffic from IPv6 address: 2001:a11::253. Modify or change your (existing) policies to allow traffic between the hosts

2) Ensure that IPv4 host 80.10.10.254 can reach IPv6 host 2001:a11::1 by sending and receiving traffic from IPv4 address 80.10.10.2 Modify or change your (existing) policies to allow traffic between the hosts

Chapter seven: Attack Prevention and Mitigation

This chapter is dedicated to the Attack Prevention and Mitigation functionality on Junos security devices. The presented tasks will require you to configure stateless packet filtering, SCREEN functionality and Intrusion Prevention System features set.

Topology for chapter seven:



You can continue with the configuration in case you have completed tasks from the chapter 3. Or you can load the latest initial configurations for this chapter to the devices.

NOTE: In case you have loaded the initial configuration for the vr-device and the access-switch before you don't have to do it again.

NOTE: The labs starting point requires to have SRX clusters formed between devices srx3 srx4 and srx5 srx6 and the respective configuration loaded on them.

TIP: Ensure you read this entire chapter, before starting with the first task.

Task 1: Firewall Filters

In this part you will configure stateless packet filters on all security devices in the lab. The goal of this task is to protect every security device's control plane from malicious traffic by applying Firewall Filters to devices loopback interfaces.

1) Ensure that IPSec tunnels can be established for all security devices in the network regardless if they are located in front of or behind NAT devices. All security devices are using ESP as an IPSec protocol.
2) Ensure that OSPF protocol is permitted for of the range of IP addresses allocated for tunnel interfaces;
3) Permit DNS on UDP port 53 and NTP traffic originated from themanagement network 10/8. Also permit the NTP from the address 172.31.10.1;
4) Permit SNMP, Radius, http/https, telnet, ssh and ftp traffic originated from the out-of-band management network 10/8;
5) Permit ping packets regardless of the source IP address;
6) Ensure that ftp and http traffic is rate limited to 1 Mbps with the allowed traffic burst of 100 KB;
7) Silently drop and syslog all other traffic.

Task 2: SCREEN

In this part you will configure lab equipment as necessary to protect network recourses of Branch offices, Finance department and Home office from different types of reconnaissance and DoS attacks with the SCREEN feature.

Branch office 1, Branch office 2, Home office: srx1, srx2 and srx8

Configure functionality on srx1, srx2 and srx8 to protect sites from malicious traffic arriving from the Core network:

1) Ensure that the SYN Proxy mechanism is enabled;
2) Protect against session table flood with the thresholds of 250 sessions per source and per destination IP addresses;
3) Configure protection against TCP SYN segments flood with the following thresholds and timer values:
    a. The destination thresholds values of 5000 TCP SYN segments per second;
    b. Ensure that security device starts SYN Proxy protection mechanism when TCP SYN segments arrival rate reaches 500 segments per second;
    c. Ensure that security device generates an alarm when TCP SYN segments arrival rate reaches 7000 segments per second;
    d. The maximum time before incomplete sessions are dropped should be 10 seconds.
4) Protect against ICMP flood with the threshold of 500 packets per second;
5) Ensure that security device drops packets with following abnormalities:
    a. Fragmented ICMP packets;
    b. Fragmented TCP SYN segments;
    c. ICMP packet with size larger than 1024 bytes;

Finance department: srx7

Configure srx7 to protect site from reconnaissance attempts arriving from the INTERNAL zone:

6) Ensure that detection of malicious traffic results in alarm generation instead of dropping the packets belonging to malicious packet flow;
7) Protect against IP addresses sweeps with a detection rate of 10 ICMP packets arrived per 500 ms time interval;
8) Protect against port scans with a detection rate of 10 port scans per 750 ms time interval;
9) Detect IP packets with following values in the Options field:
    a. Time stamp option
    b. Record route option
10) Protect against following operating systems probes:
    a. The TCP segment has both SYN and FIN flags set;
    b. The TCP segment has no flags set.

Task 3: Intrusion Prevention System

In this part you will configure lab equipment as necessary to deploy Intrusion Prevention System features in the Data Center and Central office.

Data Center: cluster1

There are several servers located in different zones in the Data Center network (see the table below). Services that are not mentioned in this table or in the following configuration tasks must be restricted by the security policies.

Security zone name	Services
TRUST	SMTP, POP3, IMAP
DMZ	HTTP, SMTP, POP3, IMAP, FTP
WAREHOUSE	HTTP

1) Configure cluster1 to use the TCP SYN cookie rather TCP SYN proxy mechanism.
2) Protect the Data Center resources with the predefined IDP policy "Recommended". Ensure that only specified services are monitored for traffic traversing between the Data Center protected resources and Untrust zone.
3) Ensure that all the Data Center resources are protected against TCP/IP attacks and malware activities from the Untrust zone as well as internal servers can't cause infection or be the source of attacks to any hosts located in the Untrust zone.
4) Allow anonymous access from Untrust zone to the ftp servers 172.16.150.1 and 172.16.150.2 only from the 80.10.1.128/29 range. Restrict access for the rest of the hosts located in the Untrust zone. Silently drop packets from unauthorized hosts, block them for 1 hour and generate log messages with severity level Major and alert flag.

Central office: cluster2

There are two servers located in the DMZ security zone in the Central office network (see table below). Services that are not mentioned in this table or in following configuration tasks must be restricted by security policies.

Server's IP address	Services
172.16.55.100	HTTP
172.16.55.200	FTP

5) Configure cluster2 to use the TCP SYN cookie rather than the TCP SYN proxy mechanism.
6) Protect the Web and the FTP servers from any kind of HTTP or FTP attacks respectively with the severity level Critical or Majorfrom everywhere. Silently drop session in the case of attack's detection, generate syslog message with the alert flag and block attacker's future connection attempts for two hours.
7) Upload of zip, rar or tgz files to the ftp server is prohibited from anywhere. Each detected attempt results in disconnecting the client from the server by receiving with TCP RST message. The client is blocked for next five minutes. The syslog message with the severity level Major must be generated. Clients located in the TRUST and in the INTERNAL zones are permitted to access servers located both in the UNTRUST zone and in the DMZ zone.

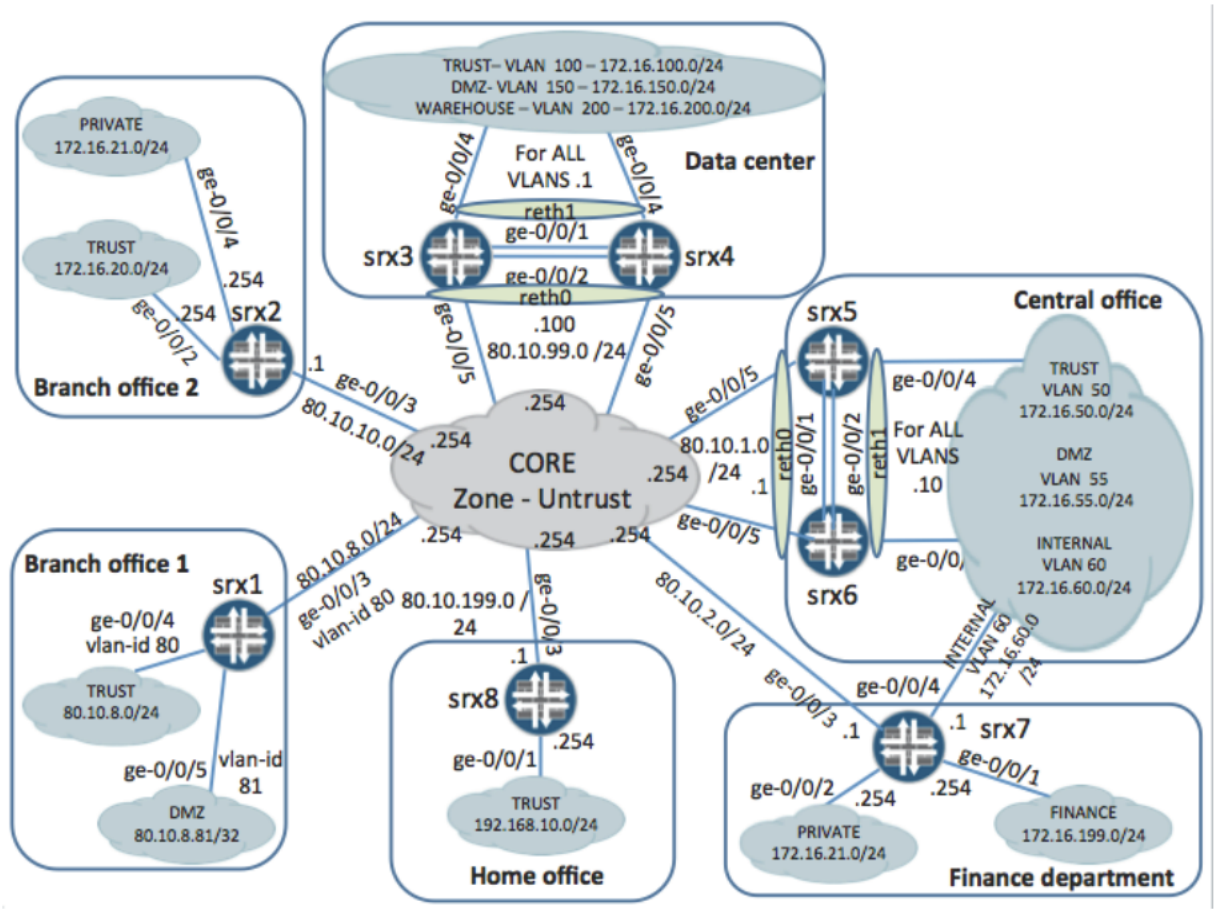
8) Ensure that client's machines located in the TRUST security zone are protected against worms and Trojans types of attacks of all severity levels from anywhere as well as they can't cause infection or be the source of attack for any hosts located in DMZ and INTERNAL security zones.
9) Clients are instantly denied access to the following URLs:
    a. www.playboy.com
    b. www.hustler.com

    The connection must be closed when such attempt is detected.
10) The downloading of pdf files via HTTP is prohibited for users located in the TRUST zone. If such attempt has been detected the connection has to be closed.

Chapter eight: Extended Implementation Concepts

This chapter is focused on two features of JUNOS Security kit: Transparent mode and Filter Based Forwarding. The presented scenarios require you to reconfigure security devices srx1 and srx7 according to picture below.

Topology for chapter eight:



You can continue with the configuration in case you have completed tasks from the chapter 7. Or you can load the latest initial configurations for this chapter to the devices.

NOTE: The initial configurations of srx1 and srx7 are **different** from final step of chapter 7. You need to download the initial configurations for these devices from our website(see link above) and load them on the srx1 and srx7.

NOTE: In case you have loaded the initial configuration for the vr-device and access-switch before you don't have to do it again.

TIP: Ensure you read this entire chapter, before starting with the first task.

Task 1: Transparent Mode

In this section you need to configure Home office's security device in such that srx1 will make forwarding decisions based on MAC address rather than on the base of IP header's information.

1) Configure the interfaces, bridge domain and security zones on the srx1 according to the table below, which reflects the topology image.
   Rewrite vlan-id 81 with the vlan-id 80 on the trunk port ge-0/0/5.0.

Interface	IP address	Interface mode	VLAN-ID	Zone
ge-0/0/4.0	N/a	Access	80	TRUST
ge-0/0/5.0	N/a	Trunk	81	DMZ
ge-0/0/3.0	N/a	Access	80	UNTRUST
irb.0	80.10.8.5/24		80	N/a

2) Configure static default route pointing to the IP address 80.10.8.254.
3) The hosts from the TRUST zone and its network range can go to the outside network (internet) with http and https.
4) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.
5) Devices in the DMZ zone should be accessible from the whole private corporate network including the local TRUST zone with https.
6) No other connections are allowed to go in or out of the TRUST zone.
7) No connections are allowed to go out from DMZ zone. Log all violations going out to the CORE network.
8) Ensure that irb.0 interface with IP address 80.10.8.5 is accessible with ping, telnet and http only from the TRUST zone.

Task 2: Filter Based Forwarding

In this section you need to configure Finance department's security device in such that srx7 will forward packets originated from PRIVATE and FINANCE zones on the based on criteria other then destination ip address.

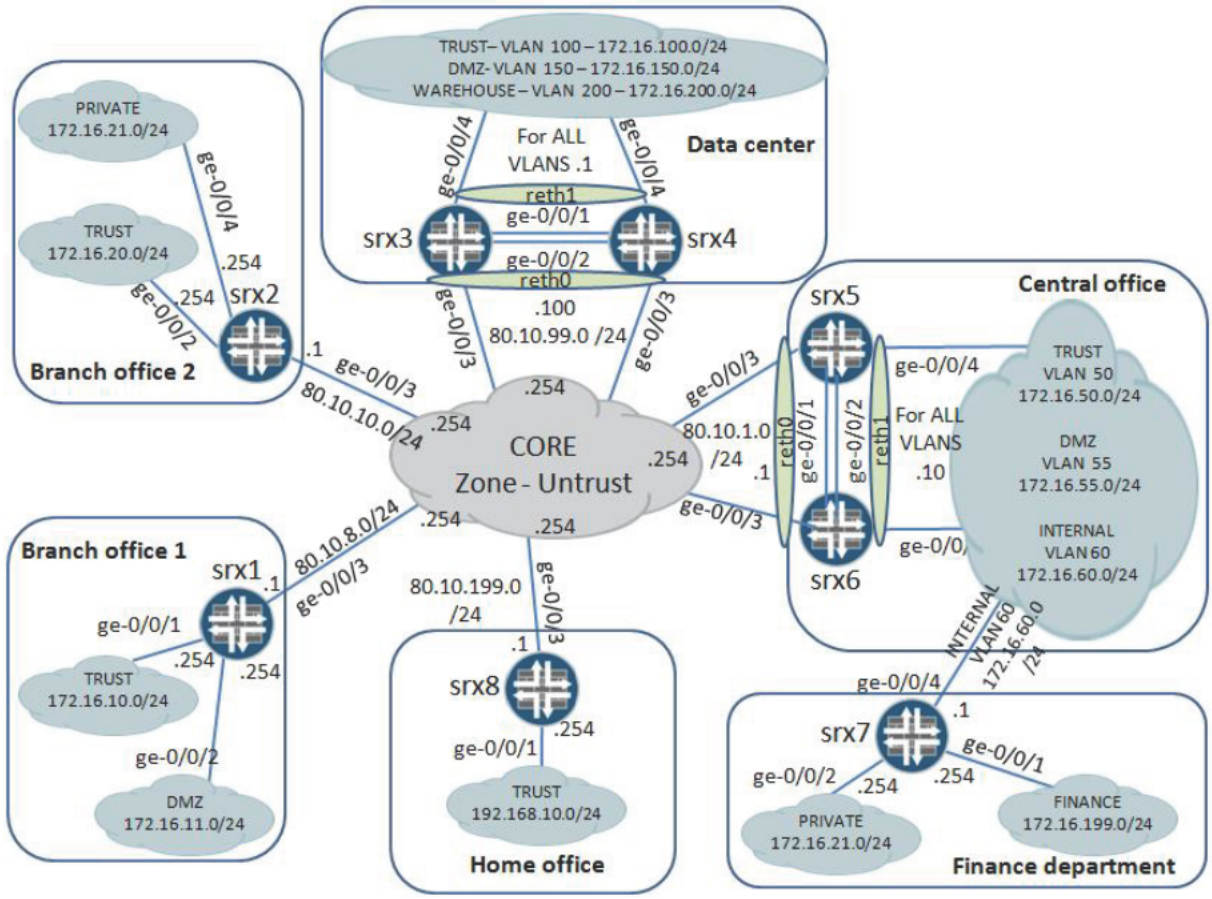
There are two network paths to the Core network available in the Finance department. One path is direct connection to the Core network via interface ge-0/0/3.0. Another path leads to the Core network via the Central office network and is formed on the base of interface ge-0/0/4.60.

1) Configure srx7 to send HTTPS traffic originated either from the PRIVATE or from the FINANCE zone and destined to the prefix 80.10.99.0/24 is forwarded via interface ge-0/0/3.0. All other traffic should be forwarded via interface ge-0/0/4.60
2) Ensure that asymmetric traffic forwarding is not possible.

Chapter nine: AppSecure

This chapter is focused on the AppSecure feature set and user identification functionality. The given tasks will have you configure the following features AppID, AppTrack, AppFW, AppQoS, SSL proxy and user identification.

Topology for chapter nine:



Load the initial configuration files for this chapter on the lab devices .

NOTE: All tasks will be performed exclusively on the cluster 1 in the data center (srx3 and srx4 devices). All configuration files except cluster 1 are the same as initial configuration files for the chapters 5, 6 and 7. But because the tasks use only cluster 1 device it is sufficient to load the start configuration only on this cluster.

NOTE: In case you have loaded the initial configuration for the vr-device and access-switch before you don't have to do it again.

TIP: Ensure you read this entire chapter, before starting with the first task.

Task 1: AppID

In this section you will adjust the parameters of the application identification on cluster 1.

Data center: cluster 1

9) Ensure the result of application identification is kept for at least 2 hours.
10) The updates have to be downloaded automatically starting from current day at 23:30 with the interval of 24 hours.

Task 2: AppTrack

Here you will configure the cluster 1 to perform application tracking in the required manner.

Data center: cluster 1

3) Deep insight is required into what applications are used by the employees in the TRUST zone. Use AppTrack to satisfy this requirement. Configure it to generate the 1^{s} message immediately when the application is identified and then to send updates every 10 minutes. Have these messages kept together with the security policy logs.

Task 3: AppFW

In this part you enable the application firewall on cluster 1 to decide whether to permit or deny a connection based on the application information rather than on the header information such as IP addresses, protocol number and ports.

Data center: cluster 1

1) Block the junos:BITTORRENT application over the port 80 from the TRUST zone to the UNTRUST zone. Define the text message for blocked sessions to be "Bittorrent is BLOCKED!!!"
2) Allow only the junos:GMAIL and junos:GOOGLETALK applications over the https port from the DMZ zone to the UNTRUST zone.
3) Ensure the firewall generates a message when the session has been denied.

Task 4: AppQoS

This section contains requirements about QoS handling where the device utilizes the knowledge about applications used in the traffic.

Data center: cluster 1

1) Ensure the loss-priority is set to high for the junos:GMAIL application from the DMZ to UNTRUST zone if it crosses 50000kb/s with bursts of 312kB in the server to client direction. In

addition have also the DSCP bit changed for the junos:GMAIL application to value of 101110 (the "ef" dscp code point alias).

Task 5: SSL Proxy

In here you will configure the cluster 1 to dive deeper and inspect also encrypted sessions.

Data center: cluster 1

1) Ensure the firewall has deep insight into encrypted sessions over the port 443 from users in the TRUST zone to the UNTRUST zone. The certificate for signing the modified server certificates should generated locally on the SRX device with following values:
   a. type: rsa
   b. key size: 1024
   c. domain name: inetzero.com
   d. subject: DC=IZ,CN=Inet-zero,OU=unit-1,O=inet-zero,SN=1234,L=Amsterdam,ST=NL,C=NL
   e. email-ID: jncie@inetzero.com
2) For server authentication use the CA certificate from the file /etc/certs/EngineeringCA.pem.
3) The connections to www.inetzero.com, www.juniper.net and www.gmail.com should be excluded from this en/decryption processing.
4) Enable logging for the allowed sessions and have it sent to the "ssl-proxy" file.

Task 6: User identification

Configure the cluster 1 to use one additional criterion user-identification in the security policy match condition.

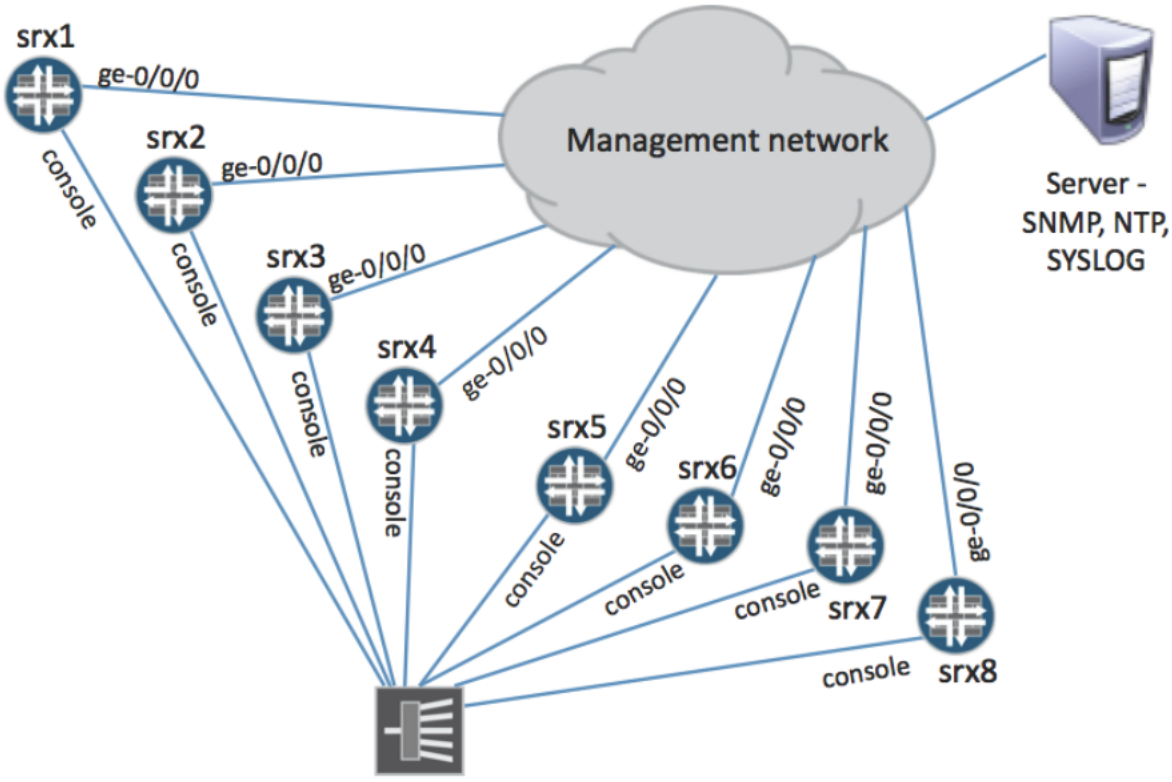
Data center: cluster 1

1) Make sure only users belonging to the group/role "jncie-sec-exam" can access the corporate network from the TRUST zone. Active Directory details are following:
   - Active Directory source priority is 25
   - Domain name: jnciesec.inetzero.com
   - Active Directory IP address: 10.10.10.10
   - BASE: DC=jnciesec,DC=inetzero,DC=com
   - user and password for Active Directory: administrator/Jncie123

Super Lab 1

This chapter lists the tasks from the Super Lab 1.

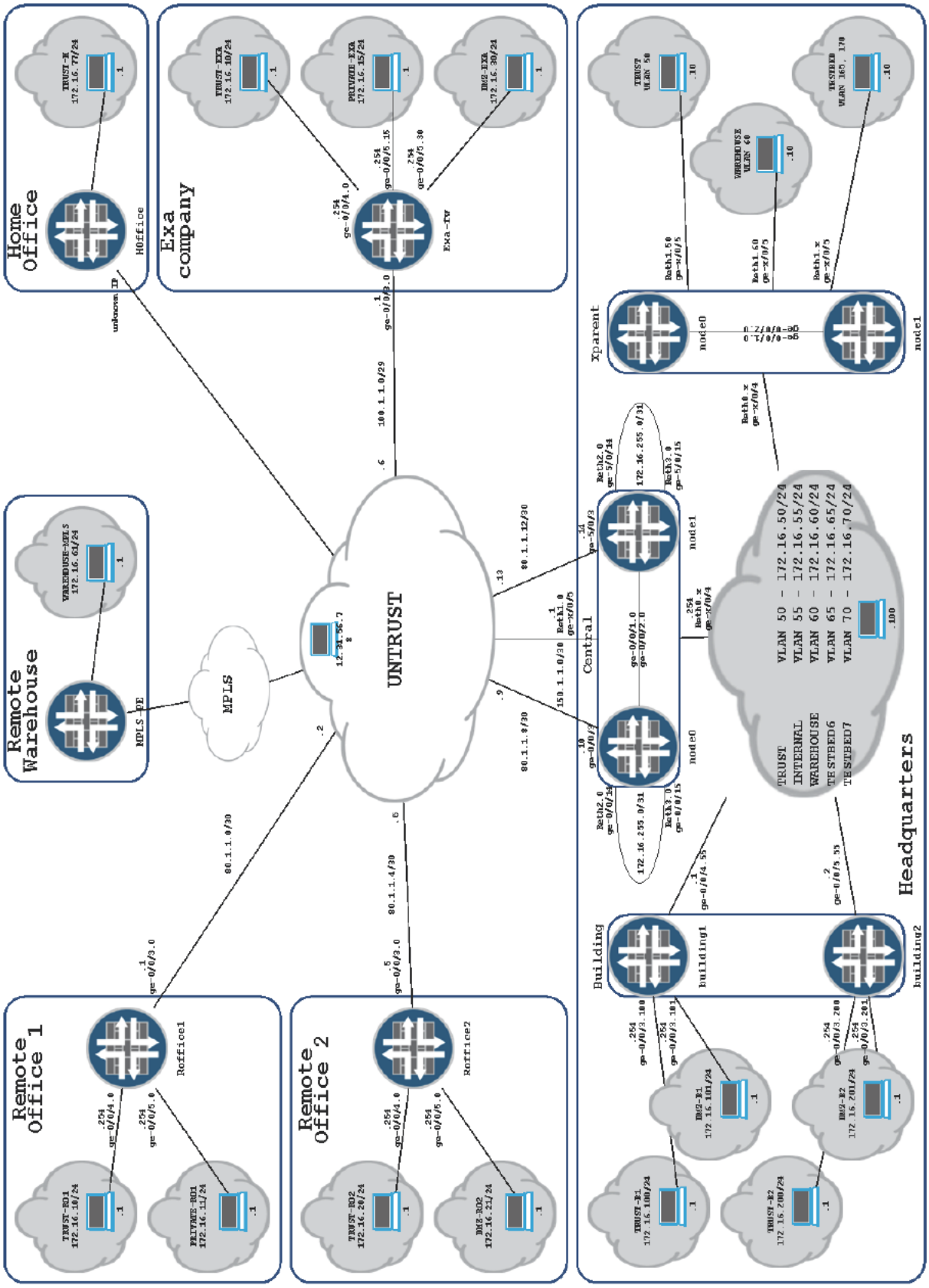
Figure1: Super Lab 1 - management network



Ensure you load the initial configurations on the devices before you start with this LAB. Ensure that you do not forget to load the initial configuration for the switches (vr-device and the access switch).

TIP: Ensure you read whole tasks before starting them.

Figure 2: Super Lab 1 topology



Task 1: Initial configuration - Part 1

In this part you will configure the device hostnames, high-availability (cluster) and management interfaces.

1) The table below lists the device hostnames mapping:

Device	Hostname
Srx1	roffice1
Srx2	roofice2
Srx3	central-node0
Srx4	central-node1
Srx5	xparent-node0
Srx6	xparent-node1
Srx7	building
Srx8	exa-fw

2) Create clusters as defined in the following table:

Device	Node ID	Cluster ID
central-node0	0	1
central-node1	1	1
xparent-node0	0	2
xparent-node1	1	2

3) Ensure ge-0/0/1 and ge-0/0/2 are used for control and fabric link respectively.

4) The routing engine of xparent cluster needs to be active on node 0

5) Configure the redundant ethernet interfaces according the figure 2.

6) Clusters should operate in the following manner:
   a. Central cluster redundancy groups mapped to interfaces dependant on physical links, need to be active on node0 whenever node0 is available
      i. Any failure from correspondent child interface triggers the failover
   b. Central cluster redundancy groups (RGs) mapped to interfaces dependant on logical links, need to be active on node1 whenever node1 is available
      i. Uplink interface monitoring triggers the failover
   c. The Central Cluster needs to monitor ICMP reachability to the host address available in the Internet. In case this reachability is compromised, the test's uplink interface should be brought down so that the RG fails over.
      i. Probe threshold should be between 30 and 60 seconds

ii. Control plane redundancy group needs to follow the same faith of the RG from poing 6.b

d. All xparent cluster redundancy groups need to be active on node 0 and should automatically failover in case any of its physical links fail.

i. No need for automatic recovery of primacy

7) Configure the management interfaces (figure 1) as defined in the table below:

Device	Management IP address
roffice1	10.10.1.1/24
roofice2	10.10.1.2/24
central-node0	10.10.1.3/24
central-node1	10.10.1.4/24
xparent-node0	10.10.1.5/24
xparent-node1	10.10.1.6/24
building	10.10.1.7/24
exa-fw	10.10.1.8/24

8) Ensure the management interfaces (figure 1):

a. Are used for management access only and won't accept any transit traffic;

b. Will accept only specific services as defined in the table below.

Device	Services
roffice1	ssh without root access (session limit 3), https
roofice2	ssh without root access (session limit 3), https
central	ssh without root access (session limit 3), https
xparent	ssh without root access (session limit 3), https
building	ssh without root access (session limit 3), https
exa-fw	ssh without root access (session limit 3), https

9) Configure a static route for the management prefix 10/8 with the gateway address of 10.10.1.254 and make sure the network is reachable if RPD is not working

Task 2: Initial configuration - Part 2

In this part you will configure authentication, authorization, Syslog, SNMP and NTP parameters.

1) Configure users as defined in the table below:

Username	Password	Device	Privileges
ronly	ronly123	All	Has permission "view" and "view-configuration". Additionally can NOT execute the "file delete" command and view the [edit system login] configuration hierarchy.
admin1	admin123	All	Has permissions "all". But is not allowed to reboot the device.
restricted	restricted123	All	Has permissions "clear" and can execute only the "show system users" and "show interface terse" commands and nothing else.
lab	lab123	All	super-user

2) Ensure that all devices have the following SYSLOG configuration:
   h. All "emergency" messages are displayed on terminals of all currently logged users.
   i. Only all "critical" and higher severity messages are sent to the default syslog file.
   j. "interactive-commands" file keeps the audit trail of the users and commands they execute.
   k. File named "security-policy-logs" will contain security policy log entries. The system should retain 20 archive files with size of 512 KB (524288 B).
   l. "authorization-file" stores authorization messages with the severity "info" and higher.
   m. Following messages are sent to the syslog server at 10.10.10.10.
      i. All "emergency" messages
      ii. Authorization messages with severity "info" and higher

3) The syslog messages should contain year and milliseconds information.

4) Ensure that all devices will synchronize their time with a NTP server reachable at 10.10.10.10.

5) The devices have to use this server's time also during booting.

6) The time zone is set to Europe/Amsterdam.

7) The ntp communication between roffice1, roffice2 devices and the ntp server needs to be protected using the MD5 authentication key number 5 and password set to "**superlab1**". These devices in turn accept only messages having the same protection.

8) All devices have to accept read-only snmp requests only from the NMS system located at 10.10.10.20. The community string is "**roaccess**".

9) All devices have to send snmp traps to the NMS system for following events:
   e. Authentication failures
   f. Hardware and environment
   g. Link transitions
   h. Routing protocol

10) The exa-fw device has to send the authentication failures to a specific monitoring system (10.10.10.50), which runs SNMP version 1 and listens on port 12345.

11) The central cluster should accept read-write SNMP requests from the network 10.10.199.0/24 except 10.10.199.199. The read-write community string is "snmpRWaccess".

12) All devices need to have defined following locations details:
   a. SNMP contact "**JNCIE admin**"
   b. SNMP description "**JNCIE-SEC device**"
   c. SNMP location "**Rack**"
   d. System location (not in the SNMP configuration): rack number **1**, floor **1**, country-code **NL**.

13) Firewall filters must protect all device's control planes in the way described below
   a. Where applicable ensure that any traffic originated from st0 or GRE interfaces is accepted;
   b. Permit DNS, NTP, SNMP, HTTPS and SSH traffic originated from subnets 10/8, 172.16/16 and 2016:abcd::/32;
   c. Ensure that ICMPv4 traffic is rate limited to 256kbps with traffic burst of 100k;
   d. Discard and syslog traffic with the protocols from 'step 15.b' for all other networks;
   e. Allow and count any other traffic from exercises where a new term is required;
   f. Silently drop all other traffic;

Task 3: Interfaces, zones, local traffic, routing and routing instances

This part is focused on the interfaces, security zones, local traffic handling, routing, routing instance segregation and device operation configurations

1) Configure interfaces and security zones on individual devices as follows (the table is based on the figure 2):

Device	Interface	IP address	VLAN-ID	Zone
roffice1	lo0.0	192.168.1.1/32	-	UNTRUST
roffice1	ge-0/0/3	80.1.1.1/30	-	UNTRUST
roffice1	ge-0/0/4	172.16.10.254/24	-	TRUST-RO1
roffice1	ge-0/0/5	172.16.11.254/24	-	PRIVATE-RO1
roffice2	lo0.0	192.168.1.2/32	-	UNTRUST
roffice2	ge-0/0/3	80.1.1.5/30	-	UNTRUST
roffice2	ge-0/0/4	172.16.20.254/24	-	TRUST-RO2
roffice2	ge-0/0/5	172.16.21.254/24	-	DMZ-RO2
central	lo0.0	192.168.1.3/32, 80.1.1.16/32	-	UNTRUST
central	ge-0/0/3	80.1.1.10/30	-	UNTRUST
central	ge-5/0/3	80.1.1.14/30	-	UNTRUST
central	reth0.50	172.16.50.254/24	50	TRUST
central	reth0.55	172.16.55.254/24	55	INTERNAL
central	reth0.60	172.16.60.254/24	60	WAREHOUSE
central	reth0.65	172.16.65.254/24	65	TESTBED
central	reth0.70	172.16.70.254/24	70	TESTBED
central	reth1.0	150.1.1.1/30	-	UNTRUST
central	reth2.0	172.16.255.0/31	-	L3VPN
central	reth3.0	172.16.255.1/31	-	WAREHOUSE
xparent	reth0.50	-	50	TRUST
xparent	reth0.60	-	60	WAREHOUSE
xparent	reth0.65	-	65	TESTBED
xparent	reth0.70	-	70	TESTBED
xparent	reth1.50	-	50	TRUST
xparent	reth1.60	-	60	WAREHOUSE
xparent	reth1.65	-	65	TESTBED
xparent	reth1.70	-	70	TESTBED
building	lo0.1	192.168.1.6/32	-	INTERNAL-B1
building1	ge-0/0/3.100	172.16.100.254/24	100	TRUST-B1
building1	ge-0/0/3.101	172.16.101.254/24	101	DMZ-B1
building1	ge-0/0/4.55	172.16.55.1/24	55	INTERNAL-B1
building	lo0.2	192.168.1.7/32	-	INTERNAL-B2
building2	ge-0/0/3.200	172.16.200.254/24	200	TRUST-B2

building2	ge-0/0/3.201	172.16.201.254/24	201	DMZ-B2
building2	ge-0/0/5.55	172.16.55.2/24	55	INTERNAL-B2
exa-fw	lo0.0	192.168.1.8/32	-	UNTRUST
exa-fw	ge-0/0/3	100.1.1.1/29	-	UNTRUST
exa-fw	ge-0/0/4	172.16.10.254/24	-	TRUST-EXA
exa-fw	ge-0/0/5.15	172.16.15.254/24	15	PRIVATE-EXA
exa-fw	ge-0/0/5.30	172.16.30.254/24	30	DMZ-EXA

2) Ping to the devices themselves must be allowed on all interfaces.

3) SSH connections are accepted on all TRUST zone interfaces.

4) On the devices roffice1, roffice2 and exa fw create a default static route pointing to the UNTRUST network.

5) Use static routes on central cluster to provide connectivity to building's networks

6) On building device create virtual router routing instances named building1 and building2, associate the interfaces of each building accordingly and create a default static route pointing to the correct VLAN interface on the central cluster.

7) Configure VLAN rewriting rules on xparent device:
   a. Interface reth1 – vlan id 165 to vlan id 65
   b. Interface reth1 – vlan id 170 to vlan id 70

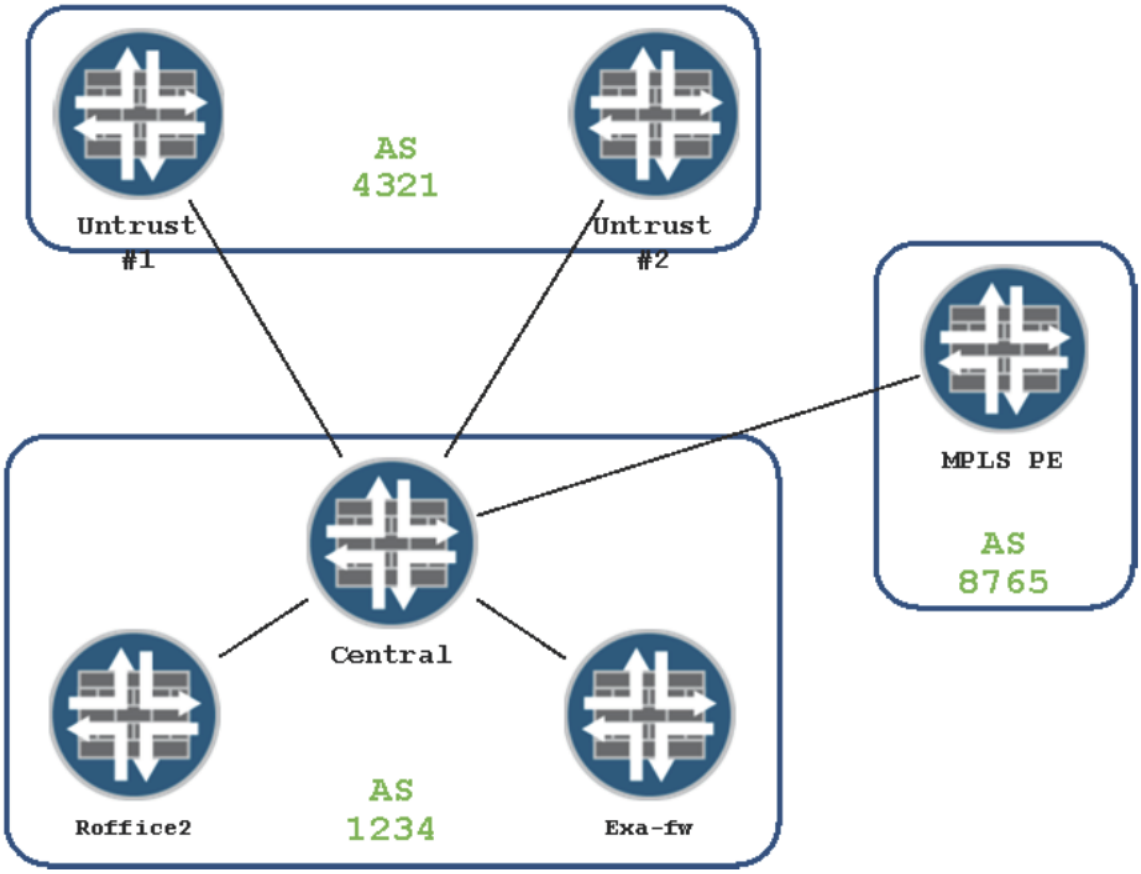
8) Configure BGP in central device to both external neighbouring addresses from ASN 4321 aided by the diagram of figure 3.
   a. Advertise the company owned prefix 80.1.1.0/24 making sure BGP prefixes do not participate in the aggregation
   b. Make sure your preferred entry and exit point for general internet connectivity is node0.

9) The central device firewall will behave as peer device (Provider Edge [PE]) for a MPLS Layer 3 VPN service. The remote PE device is identified as 'l3vpn' in the diagram.
   a. The egress MPLS enabled interface for this service is reth1.
   b. Use OSPFv2 to exchange loopback information in the backbone area so that an external MBGP / VPNv4 peering is built between both neighbours.
   c. For your MPLS signalling protocol use LDP.
   d. Create a VRF routing instance with VRF TARGET target:1234:1 and a route distinguisher of your choice.
   e. SRX support for vrf table label is limited so you will have to use an internal loop connection to forward traffic between the VRF routing instance and the

default routing instance. You are allowed to create two static routes for this task.

f. The local and remote WAREHOUSE networks need full reachability between them.

Figure 3: BGP Topology



Task 4: UTM

1) Antivirus scanning has to be done in the Remote office 1 and Remote office 2. Configure the security devices to perform antivirus scanning according to the following requirements:
   a. Only http and ftp traffic from the correspondent TRUST zones to the UNTRUST network will be scanned
   b. Full-file based scanning is done and all files and file extensions are scanned
   c. The device checks every 90 minutes for antivirus database updates
   d. The http traffic to www.internalsites.com prefix and audio mime type are excluded from antivirus scan.
   e. Compressed files are scanned up to the 3 ^{d} compression level. Files having more compression levels are dropped.
   f. Intelligent prescreening has to be enabled.
   g. The clients have to receive every 40 seconds a small portion of unchecked data to avoid timeout.
   h. The scanning engine timeout is set to 5 minutes.
   i. All fallback options are set to block except default and too-many-requests.
   j. The virus notification message is "Virus detected!"
   k. The fallback notifications are:
      i. BLOCK "AV blocked the traffic as it was not able to scan it!"

2) The exa-fw device enforces local web-filtering according the requirements below:
   a. The web filtering is done on http connections from the TRUST-EXA zone to the Internet.
   b. The following URLs are denied
      i. www.facebook.com
      ii. www.twitter.com
      iii. www.youtube.com
   c. The clients receive the "This site is not allowed" message in case their request was blocked.
   d. The local engine timeout is set to 10 minutes.
   e. All fallback options except default option block the requests.

3) In headquarters the http and ftp traffic from the TRUST zone to the internet leaving through the cluster needs to be processed in following manner:
   a. The content handling is:
      i. Cookies and java-applets are blocked
      ii. "bat" and "sh" files are blocked
      iii. The engine generates protocol error "Firewall blocked this content!" once traffic is blocked

4) In headquarters all http requests from the INTERNAL and TESTBED zones have to be redirected to the Websense V10000 appliance (172.16.60.99) located in the WAREHOUSE zone behind the XPARENT cluster firewall
   a. The Websense appliance performs proxy operation and changes the source address of the request to its own

5) The company's email server (172.16.60.199) located in the WAREHOUSE zone behind the XPARENT cluster has to be protected from these outside spammers from the Internet

   a. IP addresses: 4.4.4.4, 5.5.5.5, 45.45.45.45
   b. Domains: spam.com, bad.com
   c. Email senders: spam@gmail.com, spam@yahoo.com

Task 5: NAT

1) Following NAT translations need to be done on the roffice1 security device:
   a. The egress interface IP address is used to translate connections from the hosts in the TRUST-RO1 zone to the UNTRUST zone.
   b. The host 172.16.11.50 in the PRIVATE-RO1 zone needs to be able to receive connections from and initiate connections to the internet. The connections from internet need to be destined to the 80.1.1.64 IP address in order to reach this host.

2) NAT translation details for the roffice2 security device:
   a. Ensure the connections from the TRUST-RO2 zone to the internet are translated to 80.1.1.96-80.1.1.99 IP addresses. PAT is allowed and concurrent sessions from the same host must be translated using the same IP address.
   b. The web and database servers need to be reachable from the UNTRUST zone as defined in the table below:

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.21.2	80	80.1.1.100	8080
Database server	172.16.21.33	3306	80.1.1.100	3306

   c. Untranslated connections from the UNTRUST zone to these servers are not allowed.

3) The exa-fw device has to provide the following translations:
   a. Traffic from the TRUST-EXA hosts to the internet has to be translated to the 100.1.1.128-100.1.1.143 range. PAT is not allowed and the IP address of the egress interface has to be used when the pool is exhausted.
   b. The connections from PRIVATE-EXA hosts to the internet must be translated in following manner:
      i. 172.16.15.5 --> 100.1.1.192, 172.16.15.6 --> 100.1.1.193, …, up to 172.16.15.10 --> 100.1.1.197
      ii. Ports are not translated
      iii. Connections from other hosts are not translated
   c. The servers in the DMZ-EXA zone need to be reachable from the internet as specified in the table below:

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.30.11	80	100.1.1.3	8080
Database server	172.16.30.12	3306	100.1.1.3	3306
SSH server	172.16.30.13	22	100.1.1.4	12345

   d. Untranslated connections from the UNTRUST zone to these servers are not allowed.

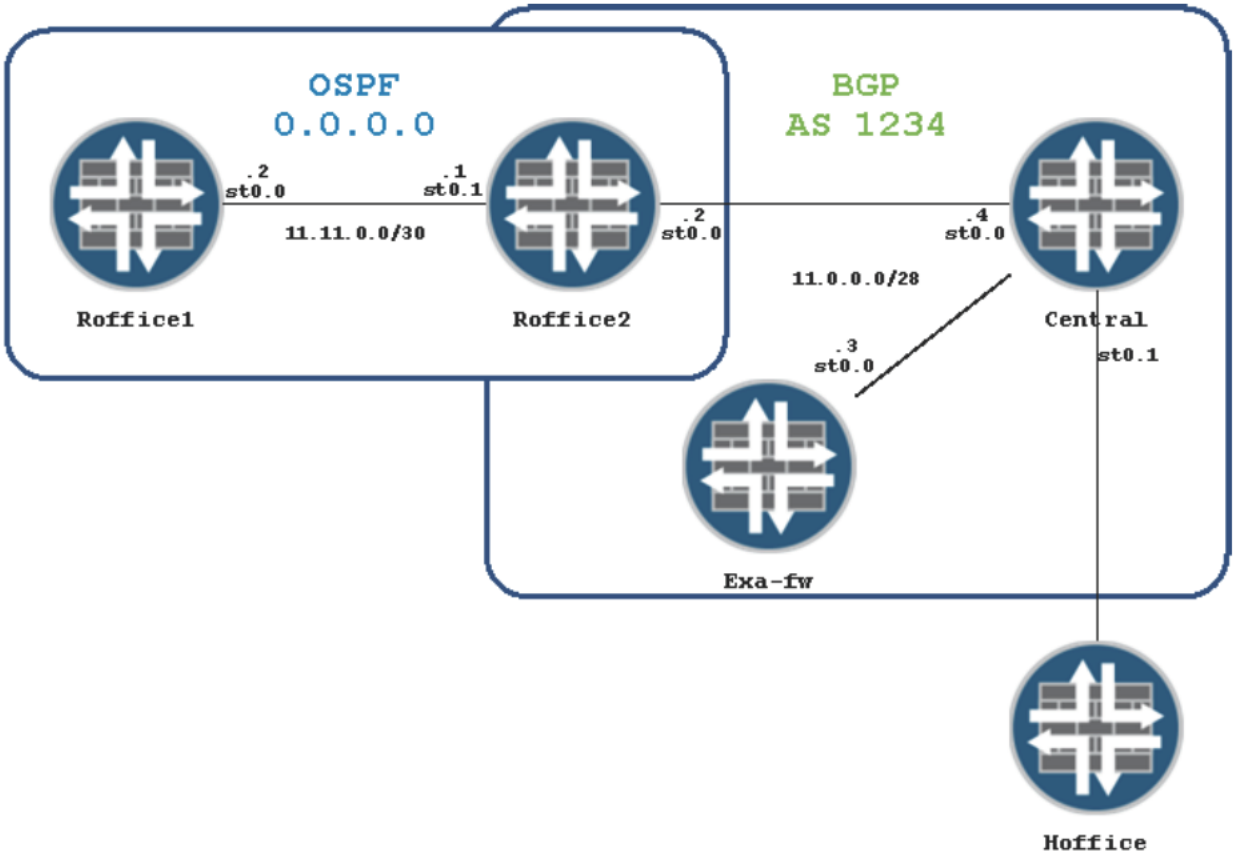
4) The connections leaving the headquarters through central cluster need to be translated in following way:
   a. All connections arriving on the cluster in the TRUST and INTERNAL zones and destined to the internet need to be translated using the 80.1.1.128 - 80.1.1.159
   b. Bidirectional translation needs to be provided for the company's email server (172.16.60.199). The public IP address allocated for this purpose is 80.1.1.192. Untranslated traffic from the UNTRUST zone to the email server must be blocked.
   c. From the WAREHOUSE zone only the Websense V10000 appliance's (172.16.60.99) initiated connections to the internet are translated. Use the 80.1.1.160 IP address.
   d. The servers located in the WAREHOUSE zone have to be reachable from the internet.

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.60.205	80	80.1.1.200	8080
Database server	172.16.60.205	3306	80.1.1.200	3306
SSH server	172.16.60.206	22	80.1.1.201	22
Honeypot	172.16.60.207	All	80.1.1.202	All

   e. Untranslated connections from the UNTRUST zone to these servers are not allowed.

Task 6: IPSec VPN

Figure 4: IPSec VPNv4



1) The VPN design between roffice1 and roffice2 assumes that the OSPFv2 needs to be run on the top of the GRE tunnel. Here are the VPN parameters that were negotiated with the roffice1 administrator:
   a. The roffice1 security device is always an initiator of the IPsec vpn. The local-id is a hostname with the value "roffice1";
   b. The st0.0 and st0.1 interfaces are used as a termination points for GRE tunnel on roffice1 and roffice2 devices respectively;
   c. The ge-0/0/3.0 interfaces are used as external interfaces for Phase 1 establishment on both sides of the vpn;
   d. IKE phase 1 proposal must include: preshared key "inetzero", 3DES, DH G1, MD5. Rekey Phase1 every 4 hours.
   e. IKE phase 2 proposal must include: AES128, ESP, DH G2, SHA1. Rekey Phase2 every hour.

f. The interfaces configuration must follow information in the table below. For the GRE tunnel source and destination address use addresses of the interfaces st0.0 on roffice1 and st0.1 on roffice2 from the table below.

Device	Interface	IP address	Zone
roffice1	st0.0	11.11.0.1/30	VPN
roffice1	gr-0/0/0.0	11.11.11.1/30	VPN
roffice2	st0.1	11.11.11.2/30	VPN
roffice2	gr-0/0/0.0	11.11.0.2/30	VPN

g. Ensure that the TRUST zone subnet of both devices appears as OSPF internal route but IGP adjacency must only be attempted across GRE interfaces.
h. Ensure that TRUST networks connected to other hosts appear as OSPF external routes.
i. Ensure that the least possible number of security policies allow the subnets located in roffice's TRUST security zones communicating to each other.

2) You need to configure an IPsec VPN between hoffice and cluster nodes. You do not have access to the hoffice device and can only use CLI for troubleshooting. Here are the VPN parameters that were negotiated with the hoffice administrator:
   a. The hoffice security device uses statically assigned public IP address. It is always an initiator of the ipsec vpn and is configured in main mode. The IP address of hoffice gateway is unknown;
   b. IKE phase 1 proposal must include: preshared key "inetzero", DES, DH G1, MD5.
   c. IKE phase 2 proposal must include: DES, ESP, MD5.

Device	Interface	IP address	Zone
central	st0.1	-	VPN

   d. The IPsec VPN should provide access for all traffic types from the TRUST-H security zone to all TRUST security zones with the least possible number of policies
   e. The remote device is prepared to negotiate phase 2 and accept traffic using the 172.16.0.0/16 network
   f. The central cluster must forward traffic into the IPSec VPN using the node that bears redundancy group primacy of the tunnel's endpoint interface.
   g. You can add a static route to reach the TRUST zone of the home-office firewall

3) The roffice2 and exa-fw security devices need to be connected to the cluster node as spokes of the hub-and-spoke VPN. Here are VPN parameters that must be used for the configuration:
   a. Only one st0 interface per security device can be used for the ipsec tunnel(s) termination;
   b. Configure the interfaces on every device according to the table below:

Device	Interface	IP address	Zone
roffice2	st0.0	11.0.0.2/28	VPN
exa-fw	st0.0	11.0.0.3/28	VPN
central	st0.0	11.0.0.4/28	VPN

c. Configure static NAT on exa-fw and cluster to solve the issue of overlapping subnets in the security zone TRUST-EXA and TRUST-RO1. Use the subnet 172.16.110.0/24 to reach the TRUST-EXA security zone network and 172.16.111.0/24 to reach the TRUST-RO1 security zone network. You can use up to two static routes.
d. Validate data path with VPN monitor option. The keepalives should be sent to the neighboring peer regardless of traffic patterns with 5 sec interval. It is allowed to miss only 3 consecutive keepalives after which the tunnel is considered inactive.
e. IKE phase 1 proposal must include: preshared key “inetzero”, AES128, DH G2, SHA1. Rekey phase 1 every 16 hours.
f. IKE phase 2 proposal must include: AES192, ESP, SHA1. Rekey phase 2 on transmission of 100 MB of traffic;
g. Configure internal BGP in the central cluster, roffice2 and exa-fw. Advertise internal network reachability using a single prefix from the central cluster.
h. Ensure all your TRUST networks from any device can communicate with each other. You must not use static routes.
i. Ensure the VPN traffic traverses the cluster member that owns priority of the VPN’s termination interface

Task 7: Attack prevention and mitigation

1) Ensure that roffice1 and roffice2 are protected against following attacks arriving from the Internet:
    a. The TCP SYN segments flooding with the following thresholds and timer values:
        i. The destination thresholds values of 10000 TCP SYN segments per second;
        ii. Ensure that security device starts SYN Proxy protection mechanism when TCP SYN segments arrival rate reaches 500 segments per second;
        iii. Ensure that security device generates an alarm when TCP SYN segments arrival rate reaches 2500 segments per second;
        iv. The maximum time before incomplete sessions are dropped should be 10 seconds;
    b. Protect against fragmented TCP SYN segments;
    c. Protect against UDP flooding with the threshold of 500 packets per second;

2) Ensure that building1 and building2 are protected against the following reconnaissance attempts arriving from the INTERNAL security zone:
    a. IP address sweep and port scan both a detection rate of 10 packets arrived per 2 ms time interval;
    b. Detect IP packets with following values in the Options field:
        i. Record-route option;
        ii. Timestamp option;
    c. Protect against following operating systems probes:
        i. The TCP segment has both SYN and FIN flags set;
        ii. The TCP segment has no flags set;
    d. Ensure that detection of malicious traffic results in alarm generation instead of dropping the packets belonging to malicious packet flow;

3) Configure cluster in such a way to protect server 172.16.60.205 and 172.16.60.206:
    a. The uploading of exe or rpm files to the 172.16.60.206 server via ftp is allowed only from the TRUST security zone and prohibited from everywhere else. Each detected attempt results in silently dropping client's sessions;
    b. Allow anonymous access to the ftp service of the 172.16.60.206 server from any TRUST and the TESTBED security zones. Restrict access for the rest of the network. Silently drop packets from unauthorized hosts, block them for 1 hour and generate log messages with severity level Major and alert flag;
    c. Protect servers against scanning and worms from the INTERNAL and TESTBED security zones. Each detected attempt results in silently dropping packets;

Task 8: AppSecure – Central cluster

1) Disable application system cache completely.

2) Enable AppTrack to provide information about applications used in the TRUST zone. The first message for each connection has to be generated 2 minutes after the application has been identified and then an update has to be created every 6 minutes.

3) Block the junos:MSN application over port 80 from the TRUST zone to the UNTRUST zone.

4) Allow only the junos:HTTP application over the default http port from the TESTBED zone into the WAREHOUSE zone.

5) Ensure session deny as well as session close messages are created for exercise 3 and 4.

6) Ensure the junos:MEGAUPLOAD application over the port 80 from the TRUST zone to the UNTRUST zone will have the loss priority of "high" if it crosses 5000 kb/s with bursts of 15000 bytes. This has to be applied in both directions - client to server and server to client.

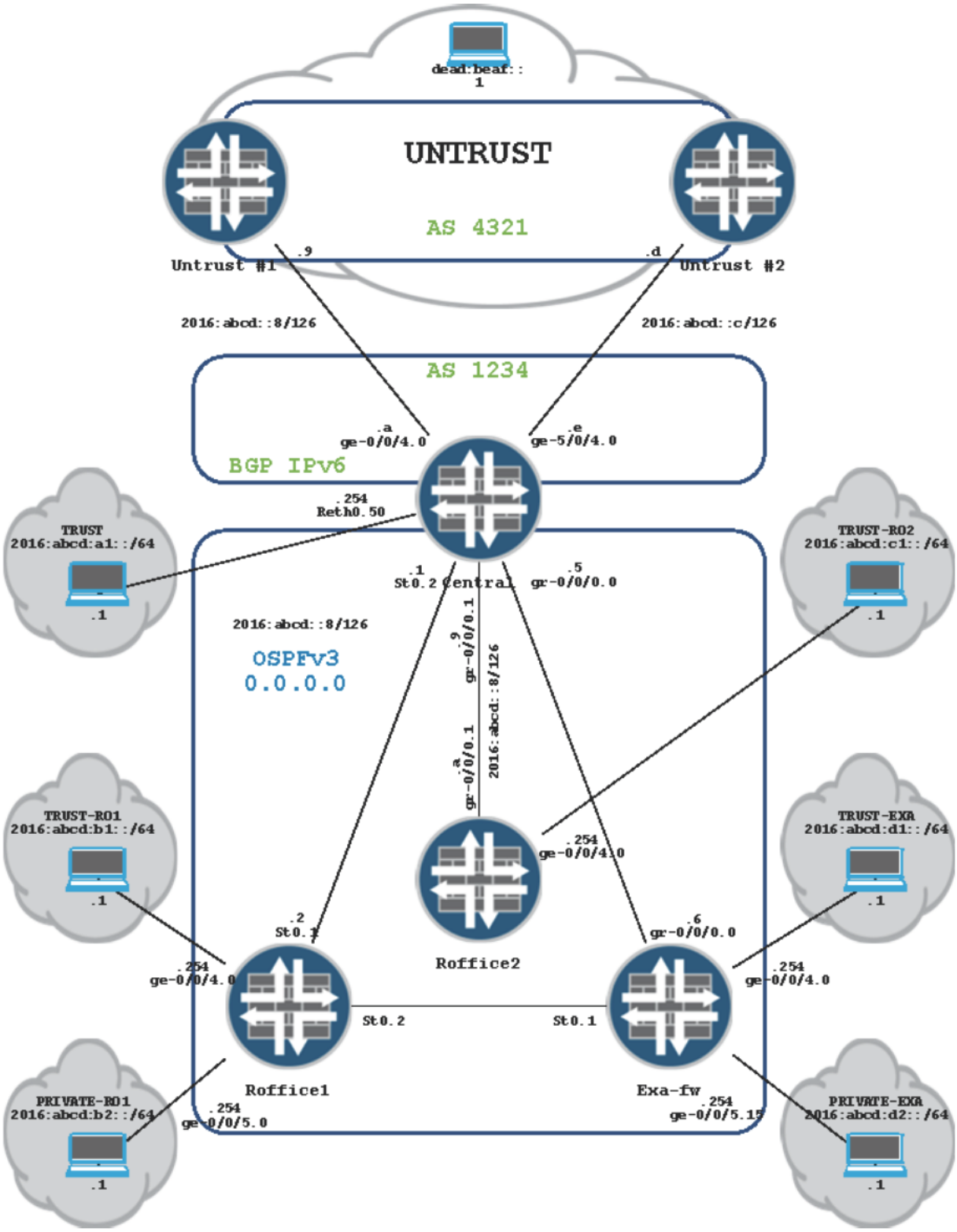
7) Make sure the SRX knows exactly what is going on in the encrypted sessions on the default https port from the TESTBED zone to the UNTRUST zone. The certificate for signing the modified server certificates should be locally generated on the SRX device with following values:
   - type: rsa
   - key size: 512
   - domain name: inetzero.com
   - subject: DC=IZ-superlab,CN=Inet-zero,OU=unit-1,O=inet-zero,SN=1234,L=Amsterdam,ST=NL,C=NL
   - email-ID: jncie@inetzero.com

   The SRX will not authenticate any servers. Make sure everything about SSL proxy operations is logged in the “ssl-proxy” file.

8) Make sure only users belonging to the group/role "superlab" can access the remote offices 1 and 2 networks from the TRUST zone. Details about the Active Directory are following:
   - Active Directory source priority is 25
   - Domain name: jnciesec.inetzero.com
   - Active Directory IP address: 10.10.10.10
   - BASE: DC=jnciesec,DC=inetzero,DC=com
   - user and password for Active Directory: administrator/Jncie123

Task 9: Extended implementation - IPv6

Figure 5: IPSec VPNv6



1) Remote offices and the newly acquired company do not have native IPv6 internet access so they have to go through the central location in a hub and spoke fashion.
   a. Central location uses native IPv6 BGP peering with existing neighbours
      i. Make sure peer #1 is preferred for incoming and outgoing traffic
      ii. Advertise the Enterprise IPv6 public prefix to these peers
   b. Use OSPFv3 between the sites for full reachability between the different IPv6 TRUST zones and HTTP reachability to the Internet.
2) Create and update existing interfaces with the following IPv6 addresses. Make sure all interfaces respond to ping requests.

Device	Interface	IPv6 address	Zone
roffice1	lo0.0	2016:abcd:ffff::2/64	UNTRUST
roffice1	ge-0/0/4.0	2016:abcd:b1::254/64	TRUST-RO1
roffice1	ge-0/0/5.0	2016:abcd:b2::254/64	PRIVATE-RO1
roffice1	st0.1	2016:abcd:eeee::2/126	VPN
roffice1	st0.2	-	VPN
roffice2	lo0.0	2016:abcd:ffff::3/64	UNTRUST
roffice2	ge-0/0/4.0	2016:abcd:c1::254/64	TRUST-RO2
roffice2	gr-0/0/0.1	2016:abcd:ffff::254/64	VPN
exa-fw	lo0.0	2016:abcd:ffff::4/64	UNTRUST
exa-fw	ge-0/0/4.0	2016:abcd:d1::254/64	TRUST-EXA
exa-fw	ge-0/0/5.15	2016:abcd:d2::254/64	PRIVATE-EXA
exa-fw	gr-0/0/0.0	2016:abcd:eeee::a/126	VPN
exa-fw	st0.1	-	VPN
central	lo0.0	2016:abcd:ffff::1/64	UNTRUST
central	ge-0/0/3.0	2016:abcd:aa01::a/126	UNTRUST
central	ge-5/0/3.0	2016:abcd:aa01::e/126	UNTRUST
central	reth0.50	2016:abcd:a1::254/126	TRUST
central	st0.2	2016:abcd:eeee::1/126	VPN
central	gr-0/0/0.0	2016:abcd:eeee::5/126	VPN
central	gr-0/0/0.1	2016:abcd:eeee::9/126	VPN

3) Configure a IPv6 over IPv4 IPSec VPN between the roffice1 device and the central cluster
   a. Phase1 and Phase 2 should use basic proposals and PSK
   b. Roffice1's external address may change

4) Use existing IPSec VPNs between Roffice2, Exa and Central devices to propagate IPv6 traffic
   a. GRE tunnels have to be used with source and destination mapped to the IPSec interface addresses

5) IPv6 private zones should have total access between roffice1 and exa fw devices

a. Create a new route based VPN associated with the unnumbered tunnel interface from the table above
b. Roffice1's external address may change
c. Use previously created basic proposals and PSK

Superlab 2

For this Superlab you have **console** access to five Juniper SRX devices. These five SRXs are part of a lab topology consisting of a cluster (***central***), one branch (***branch2***), data center devices (***datacenter*** , ***datacenter-idp***) and virus scanner (***av-scanner***).

Login to all devices with the 'lab' account and password 'lab123'.

The ***branch1*** SRX is reachable only via IPSec tunnel established between this device and ***central*** cluster. Upon completion of all tasks make sure that ***branch1*** configuration meets the requirements mentioned in this mocklab.

NOTE: Assume you **DO NOT** have access to SRX1 (***branch1***) through console or out of band.

The initial physical infrastructure is already built and devices should be preconfigured to some extent. You are **NOT** allowed to end the exam with changed preconfigured configurations with exception of the cluster devices.

You must have at least **1** task correct in each chapter. If you have all tasks incorrect for a certain chapter you automatically **fail** the entire exam.

Some tasks are depending on configurations of other tasks. For example: if a VPN is not working due to an incorrect configuration in the IGP section you will loose points for both tasks.

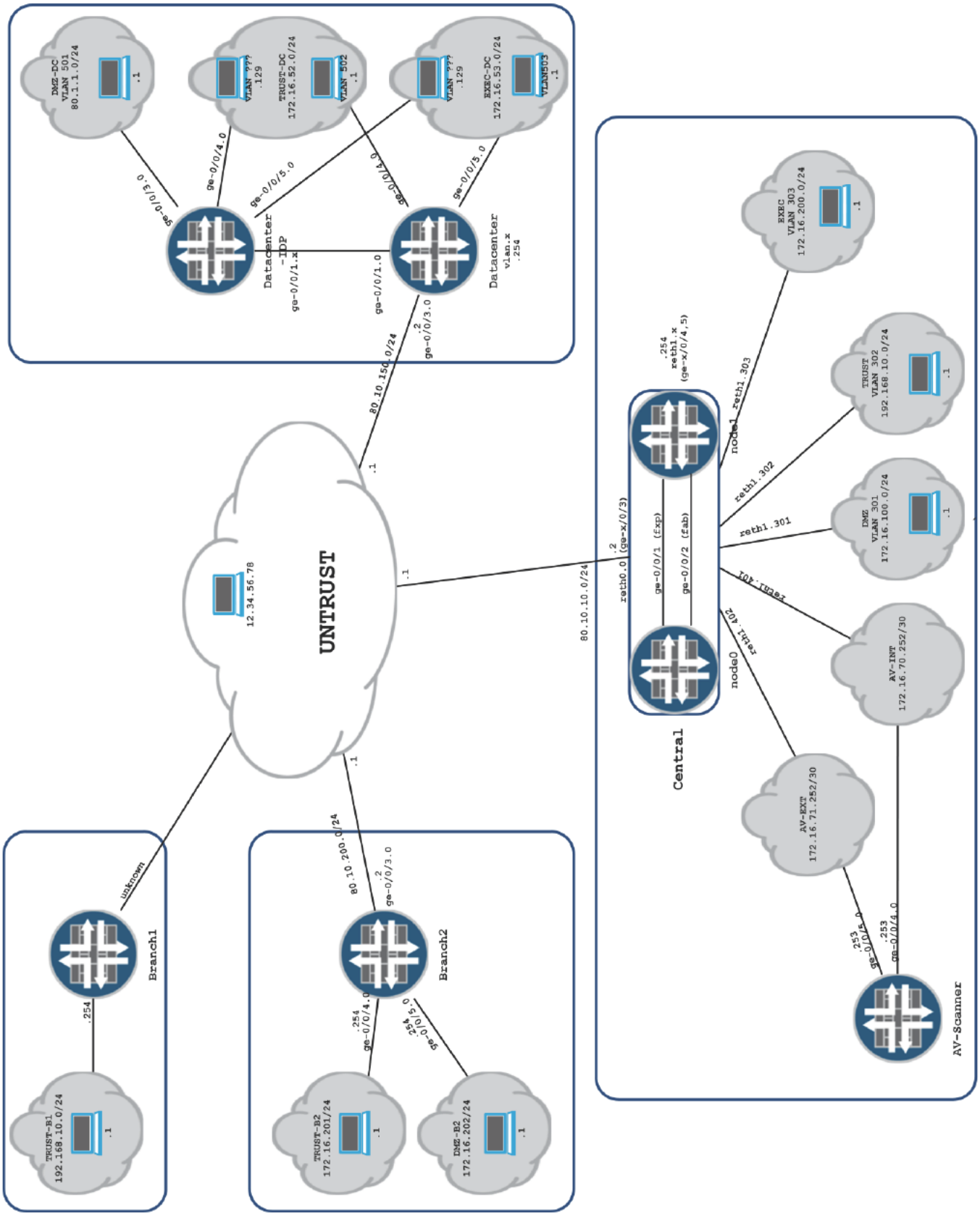
No additional static routes are allowed in the lab device's configuration unless explicitly. For each illegal static route **5** points shall be deducted of this Superlab 2 final exam score.

You are expected to deny traffic by default unless needed to complete certain tasks.

The passing score for Superlab 2 is *74* points.

During the exam you might want to verify your work by generating test traffic. You are allowed to access the ***vr-device*** and initiate test traffic through the network. The ***vr-device*** uses routing-instances to simulate the access networks as seen in your topology. Make sure if you want to send test traffic that you source from the correct routing-instance.
You are not allowed to change its configuration.

Superlab 2: Network Topology



Task 1: Infrastructure (16 points)

1.1. **3 points**

Configure chassis cluster in ***central*** with an active-passive deployment type where ***node0*** should always keep the primary state during normal operation. Ensure that the hold down interval for all redundancy groups is 10 minutes and the interfaces announces its presence with 5 ARP requests.
Use management interfaces, addresses and name conventions as mentioned in the Table 1.

1.2. **3 points**

The ***central*** device's redundant Ethernet interfaces have to be configured according to Network Topology, Table 1 and Table 2.

- Failure of any child interfaces of reth0 interfaces should cause the chassis cluster to failover to ***node1***.
- Failure of reth1 child interfaces should cause the chassis cluster's failover to ***node1*** if the available bandwidth is less than 2Gbps. Use a link control protocol.

1.3. **2 points**

Ensure that all security devices meet the criteria below:

- Add only one static route in the ***central*** device to provide reachability of hosts located in UNTRUST zone.
- Allow ping on all interfaces.
- Allow telnet and ssh only on interfaces located in management zones and lo0 interfaces. Only allow additional traffic if required for other exam tasks.

1.4. **2 point**

Configure ***datacenter*** device so that it will accept read-only SNMP requests from the network 10.10.0.0/16. The community string is "inetzero".

The ***central*** device must send snmp traps associated with link status and services to host 10.10.1.100.

1.5. **4 points**

The device ***datacenter-idp*** is preconfigured to work in transparent mode however it needs troubleshooting to make all hosts from zone TRUST-DC and EXEC-DC to communicate.

Ensure the device ***datacenter*** operates in route mode but is able to switch packets of the local attached zone with the same zone hosts behind the ***datacenter-idp*** device.

1.6. **2 points**

All security devices need to be configured so that:

- Users, passwords and authorization levels are as per Table 3.
- Sync NTP with the server located at IP address 10.10.1.100. This server should also provide the router with the time at boot up. Use Europe/Amsterdam time zone.
- DNS services are polled from IP address 10.10.1.100.
- Generate syslog according to parameters as described in Table 4.

Task 2: Security (22 points)

2.1. **3 points** Allow any host located in any TRUST zone to establish connections to HTTP and HTTPS services located in UNTRUST during working hours (8am-12am, 1pm 5pm) and only on workdays (Monday-Friday). Log all outgoing attempts that violate this policy.

2.2. **2 points** Allow any hosts located in TRUST zone of ***central*** to connect to FTP, HTTP and TELNET services located in local DMZ zone.

2.3. **2 points** Allow any host located in the UNTRUST zone to establish HTTP sessions to resources located in DMZ-DC.

2.4. **3 points** Any FTP connections to resources located in DMZ-DC from INTERNET can only be allowed if the originating IP address is authenticated by firewall pass-through authentication:

- Username = mocklab ; password = mocklab123
- Re-authentication after 1 hour of inactivity
- Banners: Login = "Welcome to InetZero!" ; Success = "Authentication successful" ; Failure = "Authentication failed"

2.5. **2 points** Ensure that every time you change security policies configuration for all devices except ***datacenter-idp*** it reflects the sessions in progress.

2.6. **5 points** There are limited device resources in the ***datacenter***. Ensure that HTTP between TRUST-DC and EXEC-DC zones skips statefull firewall inspection in the ***datacenter*** device. Ensure that ***datacenter*** security device does not require TCP SYN segments for session's creation.

2.7. **5 points** Firewall filters must protect each device's control plane in the way described below:

- Ensure that any traffic originated from any enterprise security devices is accepted.
- Ensure that SSH traffic from the management network 10.10.0.0/16 is rate limited to 512 kbps with the allowed traffic burst of 128 KB.
- Permit DNS traffic and NTP traffic originated from the address 10.10.1.100.
- No network services or protocols required in this exam may be disrupted by the application of these firewall filters.

Task 3: VPN and Routing (20 points)

3.1. **4 points**
Sites ***central***, ***branch2*** and ***datacenter*** must communicate with each other via IPSec tunnels. The topology of IPSec VPN is hub-and-spoke with ***central*** as a hub node.
All devices should use the same standard IKE Phase 1 and preshared key.
All devices should use the same basic IKE Phase 2 proposal. If the tunnel is not in use, phase 2 should time out in 30 minutes.
Only one st0 interface is allowed in each device for these IPSec tunnels.

3.2. **5 points**
The ***branch1*** device is preconfigured to initiate an IPSec tunnel to ***central*** device. You can troubleshoot the tunnel establishment process only from hub.
Use Basic Phase1 and Phase2 proposals and psk "wanna-sec-number".
As soon as connectivity is fixed you can manage ***branch1*** device by establishing a TELNET/SSH session to the ***branch1*** lo0.0 interface sourced from the local lo0.0 interface. Use a Reverse Route Injection mechanism to reach the remote loopback interface.

3.3. **2 points**
Ensure that paths of IPSec tunnels are validated with keepalive messages in 10 seconds interval regardless of user traffic. The tunnel must be considered inactive if 3 consecutive packets are missed.

3.4. **4 points**
You need to configure dynamic routing between sites ***central***, ***branch2*** and ***datacenter*** using BGP as protocol. Devices ***central*** and ***branch2*** belong to AS 65412. Device ***datacenter*** belongs to AS 65413 and establishes peering session to ***central*** device.

Ensure that traffic originated in any TRUST zone can reach any other TRUST zone via the IPSec tunnel.
Ensure that traffic originated in ***central*** EXEC zone can reach EXEC-DC zone of ***datacenter*** via IPSec tunnel.

3.5 **5 points**
The ***branch1*** device has a IPv6 host 2016:be:ef::1 that needs to access HTTP and FTP services in the IPv6 network located in the ***branch2*** device under the DMZ-B2 zone. Make sure you use the hub-and-spoke architecture and use the loopback interfaces addresses. You can add a GRE interface, assigning to the VPN zone and two static routes for this task.

Task 4: Network Address Translation (18 points)

4.1.
4 points

Ensure that hosts located in TRUST-B1 zone of ***branch1*** can establish connections to resources located in the TRUST security zone of ***central*** via IPSec VPN. Use prefixes 172.16.11.0/24 and 172.16.10.0/24 respectively to provide mapping for overlapping networks 192.168.10.0/24. Use a Reverse Route Injection mechanism to allow reachibility to remote networks.

4.2.
5 points

There are two servers located in DMZ-B2 of ***branch2***, HTTP server with Ipv6 address "2016:d0d0::8080" and FTP server with Ipv6 address "2016:d0d0::21".
Ensure that servers are reachable from INTERNET on IP addresses 80.10.200.80 and 80.10.200.21 respectively.

4.3.
5 points

Configure the ***datacenter*** device so that all sessions that are initiated from TRUST-DC, EXEC-DC zones to servers located in DMZ-DC zone appear as they are initiated from the subnet 80.1.1.128/26. PAT is allowed. Concurrent sessions from the same host must be translated using same IP address.

4.4.
4 points

Configure the ***central*** device address translation for sessions destined to INTERNET so that hosts located in TRUST zone can use up to 128 IP address from the subnet 80.10.10.0/24 starting from 80.10.10.64 for outgoing connections. PAT is not allowed. Use IP address of interface reth0.0 as a backup option. Alarm SNMP traps must be sent to host 10.10.1.100 if pool utilization raise to 75%. Alarm must be cleared if pool utilization is dropped below 60%.

Task 5: Content filtering (8 points)

5.1.
5 points

Ensure that HTTP sessions from EXEC security zone of ***central*** to resources located in the INTERNET are inspected by Kaspersky AV engine of ***av-scanner***.

The ***av-scanner*** configuration needs to meet the following requirements:

- Only scan files with extensions exe, rar, zip.
- Files with more than 3 levels of compression must be dropped.
- Engine must drop traffic if any problem occurs during antivirus scanning.
- Intelligent prescreening must be used.
- In case the AV engine needs longer time for scanning, small parts of the file should be sent to the receiver side every 100 seconds to prevent session timeout.
- User must receive a notification "Blocked by AV!" both in case of detected virus and failure to scan.

5.2.
3 points

Ensure that users' HTTP sessions from TRUST-B2 security zone of ***branch2*** to resources located in INTERNET are inspected by Surf Control Integrated web filtering engine.

branch2 needs to meet the following requirements:

- The URL's of category *Web_based_Email* must be permitted. Other categories must be blocked.
- In case the access is blocked users should receive notification message "The access is denied by security policy".
- The latest queries for web site categories should be locally cached for 30 minutes and the amount of cached data should not exceed 1KB.
- SurfControl server's address is *surfcontrolserver.com,* port *8080*.

Task 6: Attack prevention (18 points)

6.1. **5 points** Configure ***central***, ***branch1*** and ***branch2*** in such a way to provide protection against the following attacks arriving from the UNTRUST zone:

- The SYN proxy mechanism should be enabled.
- Protect against IP addresses sweeps and TCP port scans with a detection rate of 10 ICMP packets arrived per 1 second interval.
- Protect against system probes both with SYN/FIN flags set and empty TCP segment flags field.
- Protect against TCP SYN segments flooding:
    - The destination threshold value of 5000 segments per second.
    - Ensure that security device starts SYN proxy protection mechanism when TCP SYN segments arrival rate reaches 1000 segments per second.
    - Ensure that security device generates an alarm when TCP SYN segments arrival rate reaches 2500 segments per second.
    - The maximum time before incomplete sessions are dropped should be 10 seconds.

6.2. **4 points** Configure the ***datacenter-idp*** device so that servers located in the security zone DMZ-DC are protected with the following requirements:

- All HTTP attacks with severity level critical
- Upon first two attacks detection the session must be dropped and syslog message with the alert flag generated. Attacker's IP address must be blocked for 1 hour.
- Prevent uploading of .exe or .zip files via FTP
- If violation of FTP uploading policy is detected the session must be closed by sending TCP RST to the client.

6.3. **4 points** Configure Quality of Service in the ***datacenter*** device so that servers located in security zone DMZ-DC have HTTP based applications limited with the following requirements:

- All video based WEB applications rate limited to 4M with a burst of 4k.
- All audio based WEB applications rate limited to 1M with a burst of 1k.
- The traffic needs to be capped in a server to client manner.

6.4. **5 points** Enable Application Tracking in all EXEC zones. The first message should be sent 3 minutes after session creation.
Make sure that all Application Tracking events are logged with the following requirements:

- Locally in a file called 'application-tracking' restricted to 1M and 5 files
- The data with content from the security category only should be pooled from the forwarding plane and sent to host 172.16.100.1 sourcing from the EXEC zone's interface. The format of the message should be 'welf' and the severity warning and above. Name the security log stream 'APPTRACK'.

Table 1: Addressing and security zones

Device name	Rack device	Interface	IP address	VLAN-ID	Zone
central-node0	srx3	fxp0.0 (node0)	10.10.1.3/24	N/A	N/A
central-node1	srx4	fxp0.0 (node1)	10.10.1.4/24	N/A	N/A
		reth0.0	80.10.10.2/24	N/A	UNTRUST
		reth1.301	172.16.100.254/24	301	DMZ
		reth1.302	192.168.10.254/24	302	TRUST
		reth1.303	172.16.200.254/24	303	EXEC
		reth1.401	172.16.70.254/30	401	AV-INT
		reth1.402	172.16.71.254/30	402	AV-EXT
		lo0.0	192.168.1.3	N/A	VPN
		st0.0	172.16.255.1/25	N/A	VPN
		st0.1	172.16.255.254/30	N/A	VPN
av-scanner	srx5	ge-0/0/0.0	10.10.1.5/24	N/A	management
		ge-0/0/4.0	172.16.70.253/30	N/A	AV-INT
		ge-0/0/5.0	172.16.71.253/30	N/A	AV-EXT
branch1	srx1	ge-0/0/0.0	10.10.1.1/24	N/A	management
		ge-0/0/3.0	unknown	N/A	UNTRUST
		ge-0/0/4.0	192.168.10.254/24 2016:be:ef::254/64	N/A	TRUST-B1
		lo0.0	192.168.1.1	N/A	UNTRUST
		st0.0	172.16.255.253/30	N/A	UNTRUST
branch2	srx2	ge-0/0/0.0	10.10.1.2/24	N/A	management
		ge-0/0/3.0	80.10.200.2/24	N/A	UNTRUST
		ge-0/0/4.0	172.16.201.254/24	N/A	TRUST-B2
		ge-0/0/5.0	172.16.202.254/24 2016:d0d0::254/64	N/A	DMZ-B2

		lo0.0	192.168.1.2	N/A	VPN
		st0.0	172.16.255.2/25	N/A	VPN
datacenter	srx7	ge-0/0/0.0	10.10.1.7/24	N/A	management
		ge-0/0/1.0	N/A	501 502 503	N/A
		ge-0/0/3.0	80.10.150.2/24	N/A	UNTRUST
		ge-0/0/4.0	N/A	502	N/A
		ge-0/0/5.0	N/A	503	N/A
		vlan.501	80.1.1.254/24	N/A	DMZ-DC
		vlan.502	172.16.52.254/24	N/A	TRUST-DC
		vlan.503	172.16.53.254/24	N/A	EXEC-DC
		lo0.0	192.168.1.4	N/A	VPN
		st0.0	172.16.255.3/25	N/A	VPN
datacenter-idp	srx8	ge-0/0/0.0	NA	500	management
		ge-0/0/3.0	NA	501	DMZ-DC
		ge-0/0/1.0	NA	501 502 503	INTRA-DC
		ge-0/0/4.0	NA	502	TRUST-DC
		ge-0/0/5.0	NA	503	EXEC-DC
		irb.500	10.10.1.8/24	N/A	N/A

Table 2: Cluster interface mapping

Redundant Ethernet	Child Interface
reth0	ge-0/0/3
	ge-5/0/3
reth1	ge-0/0/4
	ge-0/0/5
	ge-1/0/4
	ge-1/0/5

Table 3: AAA

Username	Password	Permissions
noc	nocops123	view view-configuration

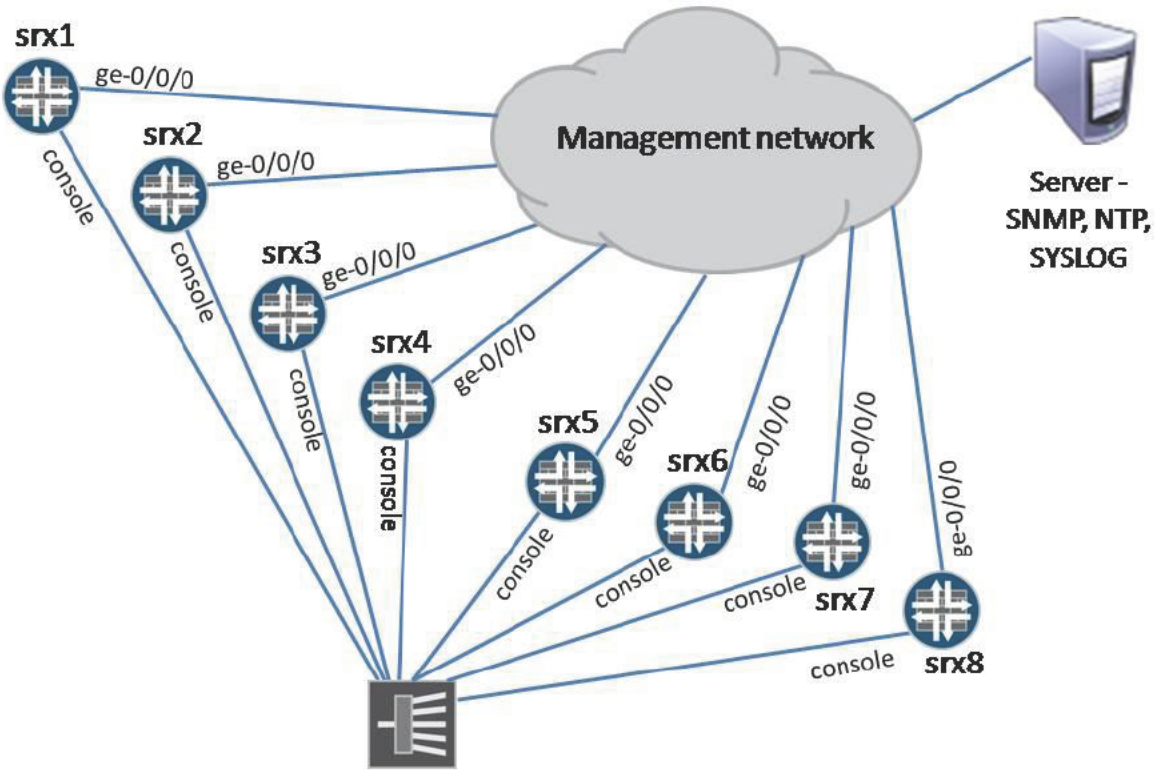
Table 4: Syslog

Destination	Type of message	Options
File: security-policy-logs	Security policies logs	Up to 5 archive files with size of 256 KB
File: watching-you	All operational/configuration commands	
Host: inetzero.com	All operational/configuration commands and configuration changes	
User: noc	Any with severity level critical or higher	

Appendix - Chapter one: General system features

This appendix provides solution details for the chapter one focused on initial system configuration and general system features.

Topology for chapter one:



Task 1: Initial configuration

NOTE: Because many tasks in this chapter require performing the same or very similar configuration on multiple devices it is suitable to use "copy and paste" approach, e.g. create the configuration on one device copy it to notepad, make changes if needed, copy it to clipboard and then paste it on other device using the "load merge terminal" or "load merge terminal relative" commands. This approach can result in significant time saving which is a huge advantage in the real exam where time is of the essence. Therefore it is advisable to use this approach whenever possible.

1) Configuring hostname is an easy task performed in the configuration mode using the following commands:

```
[edit]
root@device1# set system host-name srx1

[edit]
root@device1# commit

[edit]
root@srx1#
```

Perform the above procedure on each device and use values according to the defined table.

Device	Hostname
device1	srx1
device2	srx2
device3	srx3
device4	srx4
device5	srx5
device6	srx6
device7	srx7
device8	srx8

2) As depicted in the topology image all srx devices use the ge-0/0/0 interface for the connection to the management network, e.g.it is management interface. ge-0/0/0 and the lo0 interfaces have to be configured according the table below.

Device	Management IP address	Loopback IP address
srx1	10.10.1.1/24	192.168.1.1/32
srx2	10.10.1.2/24	192.168.1.2/32
srx3	10.10.1.3/24	192.168.1.3/32
srx4	10.10.1.4/24	192.168.1.4/32
srx5	10.10.1.5/24	192.168.1.5/32
srx6	10.10.1.6/24	192.168.1.6/32
srx7	10.10.1.7/24	192.168.1.7/32
srx8	10.10.1.8/24	192.168.1.8/32

To configure an IP address for the management and for the loopback interfaces following commands need to be used:

```
[edit]
root@srx1# set interfaces ge-0/0/0 unit 0 family inet address
10.10.1.1/24

[edit]
root@srx1# set interfaces lo0 unit 0 family inet address
192.168.1.1/32
```

Execute these commands with respective IP addresses on each device.

3) On the SRX devices which do not have dedicated hardware management interface (such as fxp0 on the high-end SRX platforms) the functional zone called "management" can be used to dedicate specific logical interface only for the management purposes.

The following commands create the functional zone called "management", associate the management interface ge-0/0/0.0 to it and enable the services listed in the given table.

```
[edit]
root@srx1# edit security zones functional-zone management

[edit security zones functional-zone management]
root@srx1# set interfaces ge-0/0/0.0

[edit security zones functional-zone management]
root@srx1# set host-inbound-traffic system-services telnet

[edit security zones functional-zone management]
root@srx1# set host-inbound-traffic system-services ssh

[edit security zones functional-zone management]
root@srx1# set host-inbound-traffic system-services http

[edit security zones functional-zone management]
root@srx1# set host-inbound-traffic system-services https
```

The configuration above allows the services only to be accessed through the interfaces associated with management zone. Enabling the service is done under the "edit system services" stanza. Following commands allow telnet, ssh with allowed root access, http and https. The https requires a certificate for operation. Either system generated certificate can be defined or a custom certificate can be loaded on the device and then used.

```
[edit]
root@srx1# edit system services

[edit system services]
root@srx1# set telnet

[edit system services]
root@srx1# set ssh root-login allow
```

```
[edit system services]
root@srx1# set web-management http

[edit system services]
root@srx1# set web-management https system-generated-certificate
```

Device	Hostname
srx1	ssh with allowed root access, telnet, http, https
srx2	ssh with allowed root access, telnet, http, https
srx3	ssh with allowed root access, telnet, http, https
srx4	ssh with allowed root access, telnet, http, https
srx5	ssh with allowed root access, telnet, http, https
srx6	ssh with allowed root access, telnet, http, https
srx7	ssh with allowed root access, telnet, http, https
srx8	ssh with allowed root access, telnet, http, https

4) The maximum connections per minute can be defined under each system service. The following commands set the limit to maximum 5 connections per minute for ssh and telnet.

```
[edit system services]
root@srx1# set telnet rate-limit 5

[edit system services]
root@srx1# set ssh rate-limit 5
```

Junos is capable to enforce limit on simultaneous connections. The configuration statement below defines that maximum 5 parallel ftp connections can be established to the system. It can be defined for ssh and telnet too.

```
[edit system services]
root@srx1# set ftpconnection-limit 5
```

Task 2: Authentication and authorization

In this part you will configure new users allowed to access the devices and define their privileges and permissions.

1) As the new user **lab** should have the super-user privileges it is sufficient to associate him with the predefined login class "super-user".

```
[edit]
root@srx1# edit system

[edit system]
root@srx1# set login user lab class super-user

[edit system]
root@srx1# set login user lab authentication plain-text-password
New password:
Retype new password:
```

2) Custom login classes need to be created as the definitions in the table below cannot be satisfied with the predefined login classes.

Username	Password	Device	Privileges
ronly	ronly123	All	Has permission "view" and "view-configuration". Additionally can NOT execute the "file delete" command.
admin1	admin123	All	Has permissions "all". Can access the configuration mode only using "configure private" command.
restricted	restricted123	All	Has permissions "clear" and execute only the "show system uptime", "show system storage" and "show interface terse" commands and nothing else.

The custom login class definition contains multiple parameters:

- permissions predefined sets of commands allowed to be executed
- allow-commands string or regular expression. Matching operational mode commands that are allowed to be executed, even if the defined permissions do not contain it
- allow-configuration - string or regular expression. Matching configuration mode commands that are allowed to be executed, even if the defined permissions do not contain it
- deny-commands string or regular expression. Matching operational mode commands that are denied
- deny-configuration - string or regular expression. Matching configuration mode commands that are denied

NOTE: Matching of the "allow-" statements is done after matching of the "deny-" statements. If a command matches both "deny-" and "allow-" statements it is allowed.

The following configuration excerpt defines the custom login classes, new users and associates them with the appropriate login class as per the table above.

```
[edit]
root@srx1# edit system login

[edit system login]
root@srx1# show
class admin-class {
    permissions all;
    allow-commands "configure private";
    deny-commands configure;
}
class restricted-class {
    permissions clear;
    allow-commands "(show system uptime)|(show system storage)|(show
interfaces terse)";
}
class ronly-users {
    permissions [ view view-configuration ];
    deny-commands "file delete";
}
user admin1 {
    class admin-class;
    authentication {
        encrypted-password "$1$NOYK1.5s$BOx9aqrmXqmYs0lAlSpe.1"; ##
SECRET-DATA
  }
}
user restricted {
    class restricted-class;
    authentication {
        encrypted-password "$1$HbJ7opMi$m4u9az/NPVWFWYj89dxcB."; ##
SECRET-DATA
    }
}
user ronly {
    class ronly-users;
    authentication {
        encrypted-password "$1$phAybng3$.mzWOja48SjPKWcXOAD2n/"; ##
SECRET-DATA
    }
}
```

Task 3: Syslog

1) The syslog configuration in Junos consists of 3 main elements destination (where the messages will be forwarded), facility (message source, e.g. who generated the message) and severity (message importance). These three elements can be repeated multiple times to achieve the desired behaviour in handling the syslog messages. The configuration shown below ensures the following behaviour in syslog messages distribution:
    n. All "emergency" messages regardless of the facility are displayed on terminals of all currently logged users.
    o. All messages regardless of the facility with the severity of "critical" and higher are sent to the default syslog file.
    p. A file named "interactive-commands" with command audit trail is maintained, i.e. file with records about the users and commands they execute.
    q. A separate file named "security-policy-logs" is used for security policy log entries. The system retains 20 archive files each with size of 512 KB (524288 B).
    r. A separate file named "authorization-file" is used for authorization messages with the severity "info" and higher.
    s. All "emergency" messages regardless of the facility are sent to the syslog server at 10.10.10.2. Non-physical address is used as source address for the syslog messages.
    t. The information about the year should be included in the messages.

```
[edit system syslog]
root@srx1# show
user * {
    any emergency;
}
host 10.10.10.2 {
    any emergency;
source-address 192.168.1.1;
}
file messages {
    any critical;
}
file interactive-commands {
    interactive-commands info;
}
file security-policy-logs {
    user info;
    match RT_FLOW;
    archive size 512k files 20;
}
file authorization-file {
    authorization info;
}
time-format year;
```

Task 4: NTP

1) The following configuration command defines a NTP server reachable at 10.10.10.3.

```
[edit system ntp]
root@srx1# set server 10.10.10.3
```

Alternatively to tell the device to use another server's time during booting instead of its own the following configuration has to be done:

```
[edit system ntp]
root@srx1# set boot-server 10.10.10.3
```

The command below tells the device to use specific source address for the ntp packets. Use appropriate IP address, e.g. loopback IP address, for each device:

```
[edit system ntp]
root@srx1# set source-address 192.168.1.1
```

2) The following command sets the time zone for the device. Be careful as this statement is NOT under [edit system ntp] but under [edit system].

```
[edit system]
root@srx1# set time-zone Europe/Amsterdam
```

3) To make the srx1, srx2 and srx8 devices use the MD5 authentication with the key set to "bootcamp" for ntp, issue following commands on each of these three devices:

```
[edit system ntp]
root@srx1# set authentication-key 1 type md5 value bootcamp

[edit system ntp]
root@srx1# set server 10.10.10.3 key 1
```

To let the devices accept only updates with the same key is done with following command:

```
[edit system ntp]
root@srx1# set trusted-key1
```

4) Defining the 2 ^{d} ntp server is pretty easy. Use the same command as in step 9) but with different IP address (10.10.10.6):

```
[edit system ntp]
root@srx7# set server 10.10.10.6
```

In order to make this server acting as the backup the other ntp server (at 10.10.10.3) needs to be defined as the preferred one.

```
[edit system ntp]
root@srx7# set server 10.10.10.3 prefer
```

5) To let the srx5 accept only authenticated messages similar configuration is needed as in step 11), just the command causing the creation of authenticated messages will be omitted.

```
[edit system ntp]
root@srx5# set authentication-key 5 type md5 value ntpserver

[edit system ntp]
root@srx5# set ntp trusted-key 5
```

Task 5: SNMP

1) The commands below define to accept read-only snmp requests only from the NMS system located at 10.10.10.4 using the community string "reading".

```
[edit snmp]
root@srx1# set community reading clients 10.10.10.4/32

[edit snmp]
root@srx1# set community reading authorization read-only
```

2) The following configuration excerpt defines to send the snmp traps listed below to the NMS system:
   i. Authentication failures
   j. Hardware and environment
   k. Link transitions
   l. Routing protocol

```
[edit snmp]
root@srx1#  show | find trap-group
trap-group test-group {
    categories {
        authentication;
        chassis;
link;
        routing;
    }
    targets {
10.10.10.4;
    }
}
```

3) This task requires creation of one more trap-group on srx1 shown below:

```
trap-group spec-monitoring {
    version v1;
    destination-port 5999;
    categories {
        link;
```

```
    }
    targets {
10.10.10.5;
    }
}
```

4) New community has to be defined on srx8. The targets here will list the network 2.2.2.0/28 and will exclude the 2.2.2.5 and 2.2.2.10 IP addresses from that range. The exclusion is achieved with the parameter "restrict".

```
[edit snmp]
root@srx8#  show | find snmpRWaccess
community snmpRWaccess {
    authorization read-write;
    clients {
        2.2.2.0/28;
        2.2.2.5/32 restrict;
        2.2.2.10/32 restrict;
    }
}
```

5) The listed commands define the SNMP contact, description and location with values "Admin user", "JNCIE-SEC device" and "Amsterdam rack" respectively.

```
[edit snmp]
root@srx1# set contact "Admin user"

[edit snmp]
root@srx1# set description "JNCIE-SEC device"

[edit snmp]
root@srx1# set location "Amsterdam rack"
```

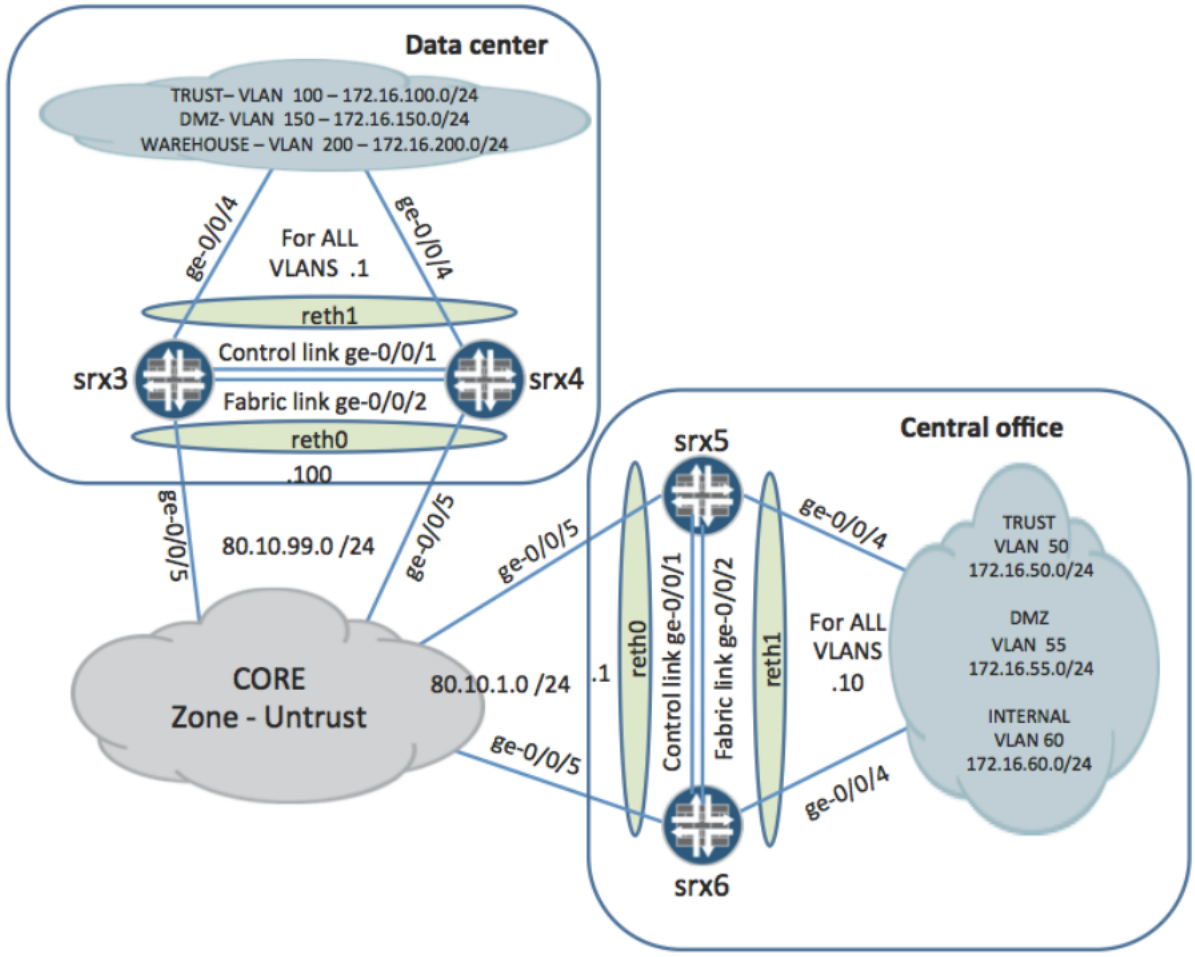
The system location details, rack number and floor are defined under [edit system location] stanza:

```
[edit system location]
lab@srx1# show
floor 1;
rack 1;
```

Appendix - Chapter two: High availability

This appendix provides details about the solution for the chapter two which is focused on system clustering.

Topology for chapter two:



Task 1: Creating clusters – initial setup

NOTE: Before executing the activities in this part ensure the configuration on all cluster nodes is prepared. The labs consist of SRX240 devices, which are branch devices and do not have dedicated management interface, such as fxp0. On the SRX branch devices in cluster setup dedicated ports (not configurable) become the management port (fxp0) and control link (fxp1) specifically on SRX 240s those are the ge-0/0/0 and ge-0/0/1 ports respectively. In order for the nodes to form the cluster successfully no configuration must exists for these interfaces in the configuration file. This allows Junos to perform internal tasks associated with these interfaces. In order to assure this execute following commands on each node of the cluster prior any cluster related tasks:

```
[edit]
root@srx3# delete interfaces ge-0/0/0

[edit]
root@srx3# delete interfaces ge-0/0/1
```

When deleting an interface configuration also all references to that interface need to be removed. From the previous chapter the functional zone "management" is referencing the interface. If there are any other references to these interfaces remove them as well.

```
[edit]
root@srx3# delete security zones functional-zonemanagement
interfaces ge-0/0/0

[edit]
root@srx3# commit
```

Failing to perform the above procedure can result in the cluster not forming correctly, i.e. the nodes will not be able to see each other (status "lost" or similar).

1) Each cluster is identified by its cluster-id (value 1-15) and consists of 2 nodes, node 0 and node 1. To create the cluster you must choose cluster-id value for it and then perform following operational mode command on each node, starting usually with node 0.

NOTE: Forming the cluster requires device's reboot. Therefore it is suitable to execute the following commands and perform the initial configuration tasks using the console connection.

Node 0:

```
root@srx3>set chassis cluster cluster-id 1 node 0 reboot
```

Node 1:

```
root@srx4>set chassis cluster cluster-id 1 node 1 reboot
```

To check the status of the cluster after the device's reboot you can use the following command:

```
{primary:node0}
root@srx3> show chassis cluster status
Cluster ID: 1
Node name         Priority   Status     Preempt Manual failover

Redundancy group: 0 , Failover count: 1
     node0      1          primary    no         no
     node1      1          secondary  no         no
```

Perform the procedure above to create clusters as the defined in table below.

Device	Node id	Cluster id
srx3	0	1
srx4	1	1
srx5	0	2
srx6	1	2

2) As mentioned earlier the branch devices have fixed definition which ports will become fxp0 and fxp1. This means the control link fxp1 is configured automatically on the lab devices. The fabric link on the other hand requires manual configuration. Based on the instructions the ge-0/0/2 ports should be used for fabric link on all clusters and their members.
As the cluster is already formed the configuration needs to be performed only on 1 member, preferably on the primary node.

NOTE: Keep in mind the interface names/numbers in cluster setup. The SRX240 has places for 4 additional PIMs, therefore the FPC number in interface names starts from value 5 on node1.

```
{primary:node0}[edit]
root@srx3# set interfaces fab0 fabric-options member-interfaces ge-
0/0/2

{primary:node0}[edit]
root@srx3# set interfaces fab1 fabric-options member-interfaces ge-
5/0/2
```

The automatic reboot of the disabled node after control link failure recovery is done using the following statement.

```
{primary:node0}[edit]
root@srx3#set chassis cluster control-link-recovery

{primary:node0}[edit]
root@srx3# commit
```

3) To configure parameters specific for each node the Junos groups need to be used and applied correctly.
The following configuration excerpt defines and applies the hostname and management IP address for the fxp0 interface on each node. The configuration excerpt is from cluster 1.

Cluster-id/Node-id	Hostname	Management IP address
1/0	srx3	10.10.1.3/24
1/1	srx4	10.10.1.4/24
2/0	srx5	10.10.1.5/24
2/1	srx6	10.10.1.6/24

To keep the configuration clean, delete the hostname configuration from the [edit system] stanza:

```
{primary:node0}[edit]
root@srx3# delete system host-name
```

Use the same approach for defining node specific parameters on cluster 2.

```
{primary:node0}[edit]
root@srx3# show groups
node0 {
    system {
        host-name srx3;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 10.10.1.3/24;
                }
            }
        }
    }
}
node1 {
    system {
        host-name srx4;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 10.10.1.4/24;
                }
            }
        }
    }
}

{primary:node0}[edit]
root@srx3#set apply-groups "${node}"
```

Configuring the loopback address is done the same way as in standalone mode (see below). However in cluster setup only one RE is active at a time and therefore hosts also the loopback interface. In case of RE failover the loopback will be moved to the new active RE.

```
{primary:node0}[edit]
root@srx3#set interfaces lo0 unit 0 family inet address
192.168.1.3/32

{primary:node0}[edit]
root@srx3# commit
```

The configuration needs to be done only on one node within the cluster. The cluster takes care of synchronizing the configurations. The following loopback addresses need to be configured on the clusters using the approach above:

cluster 1: 192.168.1.3/32

cluster 2: 192.168.1.5/32

Task2: Configuring redundancy groups and redundant ethernet interfaces

1) The RG0 is reserved for routing engines (this behavior cannot be changed). In SRX cluster every redundancy group can have priorities associated with each node. Normally the RG is active on the node with higher priority and in case of failure the RG becomes active on the other node. Upon failure recovery the failback is dependent whether the RG has the **preempt** parameter defined or not. If defined the RG will be always active on the available node with the highest priority, if not the RG will remain active on the current node. According to the task instructions the node 0 should be normally primary for the RG0 on both clusters. The following configuration excerpt performs that:

```
{primary:node0}[edit chassis cluster]
root@srx3# show redundancy-group 0
node 0 priority 200;
node 1 priority 100;
```

NOTE: The preempt parameter cannot be defined for RG0. However manual failover for RG0 is possible.

2) Based on the topology image the following reths need to be created (keep in mind the interface renaming in cluster environment).

Cluster-id	Reth	Reth children
1	reth0	ge-0/0/5, ge-5/0/5
1	reth1	ge-0/0/4, ge-5/0/4
2	reth0	ge-0/0/5, ge-5/0/5
2	reth1	ge-0/0/4, ge-5/0/4

The cluster needs to be explicitly told how many reth interfaces it should create. It might be useful to do it at the beginning of the reth configuration to prevent commit errors.

```
{primary:node0}[edit chassis cluster]
root@srx3# set reth-count 2
```

The next step is to associate the children interfaces with their parent reth interface.

```
{primary:node0}[edit interfaces]
root@srx3#set ge-0/0/5 gigether-options redundant-parent reth0

{primary:node0}[edit interfaces]
root@srx3# set ge-5/0/5 gigether-options redundant-parent reth0

{primary:node0}[edit interfaces]
root@srx3# set ge-0/0/4 gigether-options redundant-parent reth1

{primary:node0}[edit interfaces]
root@srx3# set ge-5/0/4 gigether-options redundant-parent reth1
```

Then the actual reth interface configuration remains. Based on the topology image reth0 is an IP interface without VLAN tagging and the reth1 is VLAN tagged interface (connects to 3 VLANs).

```
{primary:node0}[edit interfaces]
root@srx3#set reth0 unit 0 family inet address 80.10.99.100/24

{primary:node0}[edit interfaces]
root@srx3# set reth1vlan-tagging

{primary:node0}[edit interfaces]
root@srx3# set reth1 unit 100 vlan-id 100

{primary:node0}[edit interfaces]
root@srx3# set reth1 unit 100 family inet address 172.16.100.1/24

{primary:node0}[edit interfaces]
root@srx3# set reth1 unit 150 vlan-id 150

{primary:node0}[edit interfaces]
root@srx3# set reth1 unit 150 family inet address 172.16.150.1/24

{primary:node0}[edit interfaces]
root@srx3# set reth1 unit 200 vlan-id 200

{primary:node0}[edit interfaces]
root@srx3# set reth1 unit 200 family inet address 172.16.200.1/24
```

Perform the same procedure on cluster 2.

3) Cluster 1:
   a. To allow independent reth interface failover between nodes each reth needs to have its "own" redundancy group, i.e. each redundancy group will have only 1 reth interface associated. This means for current setup 2 RGs are needed RG1 and RG2, where RG1 will have reth0 associated and RG2 will have reth1 associated.
   b. To equally distribute the two RGs between nodes the node priorities in the redundancy groups have to be correctly specified. For example:
      i. RG1 will have node0 as primary (priority 200) and node1 as secondary (priority 100)
      ii. RG2 will have node0 as secondary (priority 100) and node1 as primary (priority 100)

      In addition the **preempt** parameter has to be defined, to ensure RG1 will be always active on node0 and RG2 on node1 in case both nodes are available.
   c. According to the setup RGs need to monitor interfaces as listed in the table below:

RG	Monitored interfaces
RG1	ge-0/0/5 , ge-5/0/5
RG2	ge-0/0/4, ge-5/0/4

As each monitored interface should cause failover their weight needs to be defined as value of 255, which is the failover threshold for redundancy groups.

The following configuration excerpt covers that:

```
{primary:node0}[edit chassis cluster]
root@srx3# show | find "redundancy-group 1"
redundancy-group 1 {
    node 0 priority 200;
    node 1 priority 100;
    preempt;
    interface-monitor {
        ge-0/0/5 weight 255;
        ge-5/0/5 weight 255;
    }
}
redundancy-group 2 {
    node 0 priority 100;
    node 1 priority 200;
    preempt;
    interface-monitor {
        ge-5/0/4 weight 255;
        ge-0/0/4 weight 255;
    }
}
```

The configuration excerpt below lists the reth interfaces configuration that the result of the commands from step 5) plus the association between reth interfaces and the respective redundancy groups:

```
{primary:node0}[edit interfaces]
root@srx3# show | find "reth0 {"
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 80.10.99.100/24;
        }
   }
}
reth1 {
vlan-tagging;
redundant-ether-options {
redundancy-group 2;
}
    unit 100 {
    vlan-id 100;
family inet {
    address 172.16.100.1/24;
}
}
    unit 150 {
    vlan-id 150;
family inet {
    address 172.16.150.1/24;
```

```
}
}
    unit 200 {
    vlan-id 200;
family inet {
    address 172.16.200.1/24;
}
}
}
```

4) Cluster 2:

d. Requirements in this case mention that the cluster scenario should be active-passive, where one node will be active and carry traffic and the other node will be standby. Therefore only one redundancy group is needed and all reth interfaces will be associated with it.

e. Because there is no need for failback needed after recovery the **preempt** parameter does not have to be defined.

f. According to the setup the RG needs to monitor all children interfaces of all reths (listed in the table below).

RG	Monitor interfaces
RG1	ge-0/0/5 , ge-5/0/5, ge-0/0/4, ge-5/0/4

As each monitored interface should cause failover their weight needs to be defined as value of 255, which is the failover threshold for redundancy group.

NOTE: Although not explicitly stated which node should be normally the primary one for the redundancy group it is advisable to define the node priorities anyway.

The following configuration excerpt covers that:

```
{primary:node0}[edit chassis cluster]
root@srx5# show | find "redundancy-group 1"
redundancy-group 1 {
    node 0 priority 200;
    node 1 priority 100;
    interface-monitor {
        ge-0/0/5 weight 255;
        ge-5/0/5 weight 255;
        ge-5/0/4 weight 255;
        ge-0/0/4 weight 255;
    }
}
```

```
{primary:node0}[edit interfaces]
root@srx5# show | find "reth0 {"
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
```

```
    unit 0 {
        family inet {
            address 80.10.1.1/24;
        }
   }
}
reth1 {
vlan-tagging;
redundant-ether-options {
redundancy-group 1;
}
    unit 50 {
    vlan-id 50;
family inet {
    address 172.16.50.10/24;
}
}
    unit 55 {
    vlan-id 55;
family inet {
    address 172.16.55.10/24;
}
}
    unit 60 {
    vlan-id 60;
family inet {
    address 172.16.60.10/24;
}
}
}
```

NOTE: As mentioned in the chapter the following step is informational as the redundancy group IP address monitoring functionality is available only on High-end SRX devices!

g. This step requires configuring the track-ip feature (or otherwise called ip address monitoring or simply ip monitoring). Cluster 2 has only one redundancy group (RG1) created as it should operate in active-passive mode. Therefore ip monitoring has to be configured for this redundancy group.

NOTE: If the ip monitoring should be configured for multiple redundancy groups use the same approach as described here.

i. Based on the requirements and on the topology image the following IP addresses should be tracked:
   - gateway (next-hop) to the CORE network --> next-hop for the default route on cluster 2 is: 80.10.1.254
   - IP address of srx7's interface from the INTERNAL zone --> 172.16.60.1

ii. The nearest reths, e.g. the reths which the cluster uses to reach these IPs, are:

- reth0.0 for 80.10.1.254
- reth1.60 for 172.16.60.1

iii. Junos security software provides the possibility to check availability of the monitored IP address also from the node where the redundancy group is in secondary state, e.g. the reth's children interfaces serve as backups. This functionality checks if the backup path works before the failover is done (as it makes no sense to do the failover if the backup path is not working too). The actual configuration is very easy, just adding for each monitored IP address the "secondary-ip-address" parameter with the correct value. Here it should be incremented IP address (by one) of the reth interface:

- for reth0.0 --> 80.10.1.2
- for reth1.60 --> 172.16.60.11

However these IP addresses need to be configured on the reth interfaces as well.

iv. Multiple ip monitoring parameters can be configured in each redundancy group that define the ip monitoring behaviour of that redundancy group.

- weight - value configured for every monitored IP address. In case of IP address failure this weight is deducted from the global-threshold
- global-weight one value defined for each redundancy group, defines the amount that is subtracted from the redundancy group failover threshold in case the global-threshold reaches 0 or negative number
- global-threshold one value defined for each redundancy group, it is the limit used to determine when the IP monitoring should contribute to the redundancy group failover threshold

NOTE: This behaviour might be bit confusing. It is important to realize that there are 2 different thresholds:

- global-threshold used ONLY for IP monitoring purposes. It is being defined for each redundancy group separately. Only when the cumulated weights of failed IP addresses reach/cross this value than the IP monitoring for affected redundancy group has failed.
- redundancy group failover threshold has value 255. The weights of failed interfaces and also the "global-weight" value (but only when the whole IP monitoring for that redundancy group has failed) are deducted from this threshold. In case result is 0 or negative number the RG failover is done.

Based on the given requirements the redundancy group failover should occur only when all monitored IP addresses fail. The following values define that behaviour:

- weights for each monitored IP 100
- global-threshold 200 --> since there are 2 monitored IP addresses each having weight of 100
- global-weight 255 --> as mentioned both failed IP addresses should trigger redundancy group failover

v. To let the redundancy group detect the failure in 8 seconds by using 4 pings, the "retry-interval" needs to be set to 2 (means every 2 seconds a new ping will be sent) and the "retry-count" to 4 (the limit for consecutive ping failures).

Here is the final configuration related to IP monitoring related for cluster 2 redundancy group 1:

```
{primary:node0}[edit chassis cluster]
root@srx5# show | find "redundancy-group 1"
redundancy-group 1 {
…
ip-monitoring{
global-weight 255;
global-threshold 200;
ip-monitoring retry-interval 2;
retry-count 5;
        family {
      inet {
                80.10.1.254{
      weight 100;
interface reth0.0 secondary-ip-address 80.10.1.2;
                 }
                 172.16.60.1{
      weight 100;
interface reth1.60 secondary-ip-address 172.16.60.11;
                 }
              }
         }
    }
}
```

Cluster checking

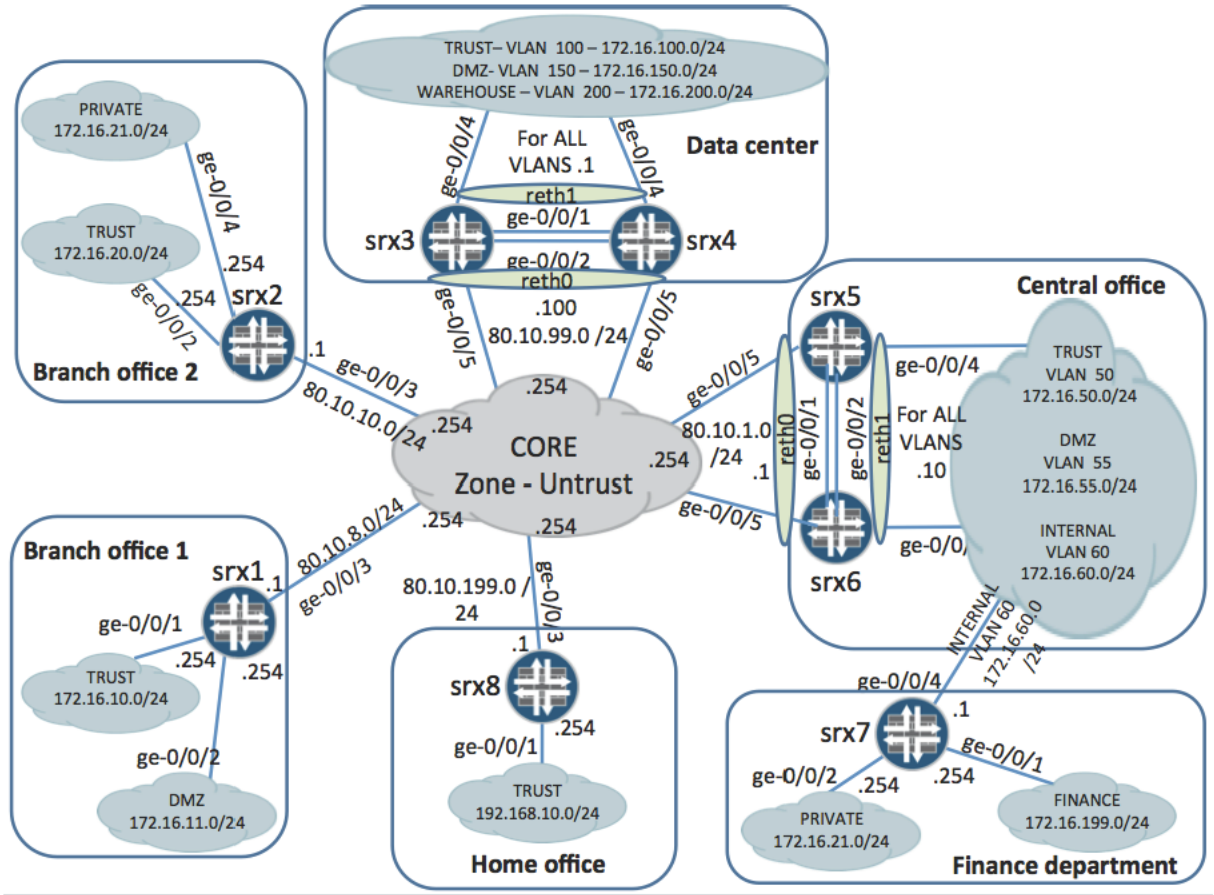
The commands below are very useful when checking the cluster, redundancy group, reth interfaces and IP monitoring status:

```
{primary:node0}
root@srx3> show chassis cluster status

{primary:node0}
root@srx3> show interfaces terse | match reth

{primary:node0}
root@srx3> show chassis cluster interfaces

{primary:node0}
root@srx3>show chassis cluster ip-monitoring status
```

Appendix - Chapter three: Firewall - Security policies

This appendix provides solution details for the security policies chapter. You will configure interfaces, zones and security policies on the SRX devices based on the requirements.

Topology for chapter three:



Task 1: Configuring interfaces and security zones

In this part you will configure interfaces, zones and assign interfaces to zones.

1) Interface configuration is pretty straightforward and no different than on any other Junos device. Below are example configuration excerpts for IP interfaces and an interface with VLANs.

```
[edit]
lab@srx7# show interfaces | find ge-0/0/1
ge-0/0/1 {
    unit 0 {
        family inet {
            address 172.16.199.254/24;
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.16.21.254/24;
        }
    }
}
ge-0/0/4 {
    vlan-tagging;
    unit 60 {
        vlan-id 60;
        family inet {
            address 172.16.60.1/24;
        }
    }
}
```

The reth interface configuration including VLANs is similar:

```
reth1 {
vlan-tagging;
    unit 100 {
    vlan-id 100;
family inet {
    address 172.16.100.1/24;
        }
    }
    unit 150 {
    vlan-id 150;
family inet {
    address 172.16.150.1/24;
        }
    }
    unit 200 {
    vlan-id 200;
family inet {
```

```
        address 172.16.200.1/24;
            }
        }
}
```

The SRX device can have 2 types of custom zones:

- Functional the name used for this zone must be "management" (no other names are allowed). Interfaces associated with this zone serve solely the management purpose and do not allow any transit traffic to pass. The management zone cannot be used in security policies configuration. Typically this zone is being used on the branch devices which do not have dedicated management port available. As this zone was already used in the chapter one here it will be skipped.
- Security user defined names are possible. Security policies are created in contexts of security zones.

The configuration below shows the association on an interface to a security zone.

NOTE: Do not forget to specify the logical unit number when associating interfaces to security zones. When omitting the logical unit number the Junos automatically uses unit 0.

```
[edit security zones]
lab@srx7# show | find security-zone
security-zone FINANCE {
    interfaces {
        ge-0/0/1.0;
    }
}
security-zone PRIVATE {
    interfaces {
        ge-0/0/2.0;
    }
}
security-zone INTERNAL {
    interfaces {
        ge-0/0/4.60;
    }
}
```

Using the approach above configure interfaces, zones and their associations according the table below.

NOTE: To save time the "copy and paste" approach might be helpful.

Device	Interface	IP address	VLAN-ID	Zone
srx1	ge-0/0/1.0	172.16.10.254/24	None	TRUST
srx1	ge-0/0/2.0	172.16.11.254/24	None	DMZ
srx1	ge-0/0/3.0	80.10.8.1/24	None	UNTRUST
srx2	ge-0/0/2.0	172.16.20.254/24	None	TRUST
srx2	ge-0/0/3.0	80.10.10.1/24	None	UNTRUST
srx2	ge-0/0/4.0	172.16.21.254/24	None	PRIVATE

Cluster1 (srx3, srx4)	reth0	80.10.99.100/24	None	UNTRUST
Cluster1 (srx3, srx4)	reth1.100	172.16.100.1/24	100	TRUST
Cluster1 (srx3, srx4)	reth1.150	172.16.150.1/24	150	DMZ
Cluster1 (srx3, srx4)	reth1.200	172.16.200.1/24	200	WAREHOUSE
Cluster2 (srx5, srx6)	reth0	80.10.1.1/24	None	UNTRUST
Cluster2 (srx5, srx6)	reth1.50	172.16.50.10/24	50	TRUST
Cluster2 (srx5, srx6)	reth1.55	172.16.55.10/24	55	DMZ
Cluster2 (srx5, srx6)	reth1.60	172.16.60.10/24	60	INTERNAL
srx7	ge-0/0/1.0	172.16.199.254/24	None	FINANCE
srx7	ge-0/0/2.0	172.16.21.254/24	None	PRIVATE
srx7	ge-0/0/4.60	172.16.60.1/24	60	INTERNAL
srx8	ge-0/0/1.0	192.168.10.254/24	None	TRUST
srx8	ge-0/0/3.0	80.10.199.1/24	None	UNTRUST

Task 2: Local traffic and static routing

1) As all interfaces should have ping allowed the best way (easy and fast) is to allow ping in each security zone in the host-inbound-traffic statement on each device. The interfaces associated with these zones will then inherit this setting.

```
[edit security zones]
lab@srx7# set security-zone FINANCE host-inbound-traffic system-
services ping

[edit security zones]
lab@srx7# set security-zone INTERNAL host-inbound-traffic system-
services ping

[edit security zones]
lab@srx7# set security-zone PRIVATE host-inbound-traffic system-
services ping
```

Do not forget to define it also for the functional zone “management” so the ping will be allowed also for the ge-0/0/0 interfaces.

2) All interfaces connected to the CORE network are assigned to the UNTUST zone as shown on the topology image. Therefore allowing the OSPF communication on these interfaces can be done by allowing the OSPF protocol in the UNTRUST zone. The exception is SRX7 which is connected to the cluster 2 and not to the CORE. On this device the OSPF communication is not needed at this time.

```
[edit security zones]
```

```
lab@srx1# set security-zone UNTRUST host-inbound-traffic
protocolsospf
```

3) Similarly as in previous step allowing ssh on all interfaces belonging to the zone TRUST can be achieved by allowing the ssh in this zone on every device.

```
[edit security zones]
lab@srx1# set security-zone TRUST host-inbound-traffic system-
services ssh
```

4) The management interface configuration was part of chapter 1. Since the ntp and snmp services were added later on the host-inbound-traffic needs to be adjusted as well to include them as well.

```
[edit security zones]
lab@srx1# show
functional-zone management {
    interfaces {
        ge-0/0/0.0;
    }
    host-inbound-traffic {
        system-services {
ping;
ssh;
            telnet;
            http;
            https;
            snmp;
            ntp;
        }
    }
}
```

Also the snmp needs to be added to the srx8 host-inbound traffic configuration for the UNTRUST zone to allow connections from the 2.2.2.0/28 networks as they arrive in this zone.

```
[edit security zones]
lab@srx8# show
...
security-zone UNTRUST {
    interfaces {
      ge-0/0/3.0;
    }
    host-inbound-traffic {
      system-services {
          ping;
          snmp;
      }
       protocols {
          ospf;
      }
    }
}
```

5) The static default route has 0.0.0.0/0 as the destination network and the next hop IP address is different for every device. It depends on the interface facing the CORE network. To configure default static route on each device execute following command on each device with correct next hop value.

```
[edit]
lab@srx1# set routing-options static route 0.0.0.0/0 next-hop
80.10.8.254
```

In this topology the srx7 device is specific as it is not directly connected to the CORE network. The traffic has to go through the cluster 2. Therefore the default route on the srx7 has as the next-hop the IP address of the reth1.60 interface on cluster 2.

```
[edit]
lab@srx7# set routing-options static route 0.0.0.0/0 next-hop
172.16.60.10
```

6) To provide connectivity for the FINANCE zone in the Finance department through the cluster 2 the following static route needs to be created on cluster 2.

```
{primary:node0} [edit]
lab@srx5# set routing-options static route 172.16.199.0/24 next-hop
172.16.60.1
```

7) The following static route provides connectivity to the management network 10/8 using the given next-hop. This static route is the same on all devices. The “copy and paste” approach can speed up the configuration process.

```
[edit]
lab@srx1# set routing-options static route 10/8 next-hop 10.10.1.254
```

Task 3: Security policies

The table below lists the values referenced in the tasks.

Name	Network range
Private corporate network	172.16/16
Internet	0.0.0.0/0

The resulting security policies that need to be created are presented tabular form, containing the device, zone context (incoming zone, outgoing zone), address books values,applications and actions. In addition for some security policies a brief description/explanation is provided.

The actual configuration (address entries, address-sets, applications, application-sets, security polices and additional needed configuration) for each device is provided at the end of this appendix chapter.

NOTE: The names for the address entries in the actual configurations can be arbitrary, but it is recommended to keep them meaningful. In addition it is essential the address entries and address-sets are created in the appropriate zones.

NOTE: Another very important thing to keep in mind is the order of security policy execution the order in which they appear in the configuration defined the sequence of execution. Every time a new security policy is created in a given context of incoming zone to outgoing zone, it is always placed at the end in that context and many times reordering is needed. The command "insert" is used for policy reordering.

Branch office 1: srx 1

1) The hosts from the TRUST zone and its network range can go to the outside network (internet) with http and https.
   To avoid creation of multiple policies an application-set can be used to group junos-http and junos-https applications.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx1	TRUST	UNTRUST	172.16.10.0/24	Any	junos-http junos-https	permit

2) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx1	TRUST	UNTRUST	172.16.10.0/24	172.16.0.0/16	any	permit

3) Devices in the DMZ zone should be accessible from the whole private corporate network including the local TRUST zone with https.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx1	UNTRUST	DMZ	172.16.0.0/16	172.16.11.0/24	https	permit
srx1	TRUST	DMZ	172.16.10.0/24	172.16.11.0/24	https	permit

4) No other connections are allowed to go in or out of the TRUST zone.
Since the devices are firewalls which drop not explicitly allowed traffic by default, no security policy is needed here.
5) No connections are allowed to go out from DMZ zone. Log all violations going out to the CORE network.
As mentioned before the firewalls drop not explicitly allowed traffic by default which means no security policy might be needed here to drop the traffic. But in order to log all violations a security policy has to be defined having the action "log".

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx1	DMZ	UNTRUST	Any	Any	any	deny log

Make sure this security policy is last in the context of incoming zone DMZ to outgoing zone UNTUST.

Branch office 2: srx2

6) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx2	TRUST	UNTRUST	172.16.20.0/24	172.16.0.0/16	any	permit

7) No other connections are allowed in or out of the TRUST zone. Log all outgoing violations to the destinations reachable via the CORE network.
As only the outgoing connections need to be logged one security policy for them has to be created. The incoming connections are dropped by default.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx2	TRUST	UNTRUST	172.16.20.0/24	Any	any	deny log

Make sure this security policy is last in the context of incoming zone TRUST to outgoing zone UNTUST.

8) Hosts from the PRIVATE zone can connect to the DMZ zone in the Central office and Data center using ssh, http, https, ftp, telnet.
To make connections from the PRIVATE zone to the rest of the network possible NAT needs to be performed. Due the fact the NAT is being performed separately from security policies in Junos firewalls the security polices can be defined also at this moment. Because the source NAT translation is done after the security policies the addresses referenced are the original addresses of the received packets.
In addition to avoid creation of multiple security policies the address-sets and application-sets should be used.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx2	PRIVATE	UNTRUST	172.16.21.0/24	172.16.150.0/24 172.16.55.0/24	junos-ssh junos-http junos-https junos-ftp junos-telnet	permit

Home office: srx8

9) Hosts connected to the srx8 can access the whole private corporate network regardless of the application and in addition have http and https permitted to the outside world/internet.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx8	TRUST	UNTRUST	192.168.10.0/24	172.16.0.0/16	any	permit
srx8	TRUST	UNTRUST	192.168.10.0/24	Any	junos-http junos-https	permit

Finance department: srx7

10) From the FINANCE zone all connections are allowed to the INTERNAL zone and to the WAREHOUSE zone in the Data center only for SQL queries. The database server in Data center listens on ports 5000 6000. Ensure the appropriate ALG for SQL is being used.
In this case a custom application needs to be defined:

```
[edit]
lab@srx7# show applications
application custom-sql {
    application-protocol sqlnet-v2;
    protocol tcp;
    destination-port 5000-6000;
}
```

Device	Incoming	Outgoing	Source address	Destination	Application	Action

	zone	zone	entry	address entry		
srx7	FINANCE	INTERNAL	172.16.199.0/24	172.16.60.0/24	any	permit
srx7	FINANCE	INTERNAL	172.16.199.0/24	172.16.200.0/24	custom-sql	permit

11) DMZ zones in the Data center and Central office are reachable from the FINANCE zone using http, https and ssh.
The access to the DMZ zones in Data center and Central office is via the INTERNAL zone.
Also here to avoid creation of multiple security policies the address-sets and application-sets should be used. However the requirement to allow only specific applications prevents the merging with the defined in the previous step.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx7	FINANCE	INTERNAL	172.16.199.0/24	172.16.150.0/24 172.16.55.0/24	junos-http junos-https junos-ssh	permit

Data center: cluster1

12) The TRUST zone has access to the whole private corporate network (also locally connected networks) with any application.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster1	TRUST	UNTUST	172.16.100.0/24	172.16.0.0/16	any	permit
cluster1	TRUST	DMZ	172.16.100.0/24	172.16.150.0/24	any	permit
cluster1	TRUST	WARE HOUSE	172.16.100.0/24	172.16.200.0/24	any	permit

13) No other connections are allowed in or out of the TRUST zone. Log all outgoing violations, e.g. connections going to CORE network.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster1	TRUST	UNTRUST	172.16.100.0/24	any	any	deny log

Make sure this security policy is last in the context of incoming zone TRUST to outgoing zone UNTUST.

14) Full communication between DMZ (local and central office) and WAREHOUSE zone is possible in both directions.
The full communication here means any application. The access to the DMZ zone in the Central office here goes through the UNTRUST zone.

Device	Incoming	Outgoing	Source address	Destination	Application	Action

	zone	zone	entry	address entry		
cluster1	DMZ	WARE HOUSE	172.16.150.0/24	172.16.200.0/24	any	permit
cluster1	WARE HOUSE	DMZ	172.16.200.0/24	172.16.150.0/24	any	permit
cluster1	WARE HOUSE	UNTRUST	172.16.200.0/24	172.16.55.0/24	any	permit
cluster1	UNTRUST	WARE HOUSE	172.16.55.0/24	172.16.200.0/24	any	permit

15) Http, https, ssh, smtp, ftp and telnet connections from the private corporate network (reachable via CORE network) to DMZ are allowed.
Also this security policy should utilize application-set.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster1	UNTUST	DMZ	172.16.0.0/16	172.16.150.0/24	junos-http junos-https junos-ssh junos-smtp junos-ftp	permit

16) Only the specific SQL connections (described previously) from the FINANCE zone in the Finance department are allowed to enter the WAREHOUSE zone. Count this traffic.
Counting traffic handled by specific policy is achieved using the action "count". The actual counters can be examined using the "show security policies …. detail" command.
As in case of Finance department also here the custom application needs to be created with the same parameters:

```
applications {
application custom-sql {
application-protocol sqlnet-v2;
protocol tcp;
destination-port 5000-6000;
}
}
```

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster1	UNTUST	WARE HOUSE	172.16.199.0/24	172.16.200.0/24	custom-sql	permit count

Central office: cluster2

17) Ensure the permitted connections from the Finance department on the srx7 are allowed as well, but focus only network ranges and not applications, i.e. when defining these policies disregard the applications.

Brief recap: in Finance department the following connections are allowed (listing only source zone/device and destination zone/device):

- FINANCE (srx7) --> INTERNAL (srx7)
  - No need for security policy on cluster 2 as this traffic is not traversing the cluster 2.
- FINANCE (srx7) --> WAREHOUSE (cluster1)
  - Security policy is needed, locally on the cluster 2 this traffic is received in the zone INTERNAL and goes out through the zone UNTRUST.
- FINANCE (srx7) --> DMZ (cluster1)
  - Security policy is needed, locally on the cluster 2 this traffic is received in the zone INTERNAL and goes out through the zone UNTRUST.
  - This security policy can be merged with the previous one.
- FINANCE (srx7) --> DMZ (cluster2)
  - Security policy is needed, locally on the cluster 2 this traffic is received in the zone INTERNAL and goes out through the zone DMZ.

As the applications can be disregarded the security policies will use "any" for the application.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	INTERNAL	UNTRUST	172.16.199.0/24	172.16.150.0/24 172.16.200.0/24	any	permit
cluster2	INTERNAL	DMZ	172.16.199.0/24	172.16.55.0/24	any	permit

18) Hosts located in the INTERNAL zone have full access to the local DMZ resources but only during working days and working hours (8:00 - 18:00).
For this purpose a scheduler active only during working days and defined hours needs to be created and then associated with the security policy.
The scheduler definition is following:

```
schedulers {
    scheduler working-time {
        daily {
            start-time 08:00:00 stop-time 18:00:00;
        }
        sunday exclude;
        saturday exclude;
    }
}
```

The following scheduler definition is correct too:

```
schedulers {
    scheduler working-time {
        monday {
            start-time 08:00:00 stop-time 18:00:00;
        }
        tuesday {
            start-time 08:00:00 stop-time 18:00:00;
```

```
            }
            wednesday {
                start-time 08:00:00 stop-time 18:00:00;
            }
            thursday {
                start-time 08:00:00 stop-time 18:00:00;
            }
            friday {
                start-time 08:00:00 stop-time 18:00:00;
            }
        }
    }
```

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	INTERNAL	DMZ	172.16.60.0/24	172.16.55.0/24	any	permit scheduler

19) The TRUST zone has access to the whole private corporate network (also locally connected networks) with any application. In addition only http and https access is allowed to the internet from the TRUST zone. Log all outgoing violations, e.g. connections leaving the cluster through the UNTRUST zone.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	TRUST	UNTRUST	172.16.50.0/24	172.16.0.0/16	any	permit
cluster2	TRUST	DMZ	172.16.50.0/24	172.16.55.0/24	any	permit
cluster2	TRUST	INTERNAL	172.16.50.0/24	172.16.60.0/24 172.16.199.0/24 172.16.21.0/24 Or use here the corporate network 172.16.0.0/16	any	permit
cluster2	TRUST	UNTRUST	172.16.50.0/24	any	junos-http junos-https	permit
cluster2	TRUST	UNTRUST	172.16.50.0/24	any	any	deny log

Make sure this security policy is last in the context of incoming zone TRUST to outgoing zone UNTUST.

20) Full communication between DMZ and WAREHOUSE zone is possible in both directions.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	DMZ	UNTRUST	172.16.55.0/24	172.16.200.0/24	any	permit
cluster2	UNTRUST	DMZ	172.16.200.0/24	172.16.55.0/24	any	permit

Ensure respective policies are present on the cluster 1 (look for these entries):

Device	*Incoming zone*	*Outgoing zone*	*Source address entry*	*Destination address entry*	*Application*	*Action*
cluster1	*WARE HOUSE*	*UNTRUST*	*172.16.200.0/24*	*172.16.55.0/24*	*any*	*permit*
cluster1	*UNTRUST*	*WARE HOUSE*	*172.16.55.0/24*	*172.16.200.0/24*	*any*	*permit*

21) Http, ftp and telnet requests sourced from the private corporate network arriving on the core network facing interface and destined to the DMZ hosts need to be authenticated in order to be granted. Use the pass-through authentication with following settings
    a. username: testuser, password: testuserpw123
    b. 1 hour of inactivity will result in re-authentication
    c. the password are stored locally on the security device
    d. ftp and telnet banners:
        i. initial banner: "Look out firewall authentication!!!"
        ii. in case of successful authentication: "Correct!"
        iii. in case of unsuccessful authentication: "Incorrect!"

    The pass-through authentication is one of 2 options of the firewall authentication. It is applicable ONLY to clear text protocols: telnet, ftp and http and no others. The firewall here intercepts the communication between the end hosts and asks for authentication inline. The other option is the web-authentication, which can be used also for other protocols and applications. In this case the user needs go to defined IP address on the firewall using browser and authenticate there. Only upon successful authentication the connections to the desired destinations will be granted.
    To configure the firewall to perform an authentication in security policy following things are needed:

    - an access profile
        - in case of local authentication also the clients and passwords need to be defined locally on the device
        - idle timeout for enforcing re-authentication after defined inactivity period
    - firewall and pass-through authentication settings
        - banners
        - which access profile to use
    - configure in the security policy permit action to perform pass-through authentication and specify which clients are allowed to use the policy by defining the "**client-match**" parameter

```
access {
    profile FWauth {
        authentication-order password;
        client testuser {
            firewall-user {
```

```
                password
"$9$Sm9yMXVb2aGiYgF/tpEhevWXdsYgJkmTJZn/tpB1"; ## SECRET-DATA
            }
        }
        session-options {
            client-idle-timeout 60;
        }
    }
    firewall-authentication {
        pass-through {
            default-profile FWauth;
            ftp {
                banner {
                    login "Look out firewall authentication!!!";
                    success "Correct!";
                    fail "Incorrect!";
                }
            }
            telnet {
                banner {
                    login "Look out firewall authentication!!!";
                    success "Correct!";
                    fail "Incorrect!";
                }
            }
        }
    }
}
```

Configuration excerpt from the security policy which performs the pass-through authentication:

```
then {
permit {
     firewall-authentication {
pass-through {
client-match testuser;
    }
}
}
}
```

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	UNTRUST	DMZ	172.16.0.0/16	172.16.55.0/24	junos-http junos-ftp junos-telnet	permit, firewall-authentication

22) Ssh and https connections from private corporate network arriving on the core network facing interface and destined to the DMZ hosts the are granted without authentication.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action

cluster2	UNTRUST	DMZ	172.16.0.0/16	172.16.55.0/24	junos-https junos-ssh	permit

Troubleshooting

Testing and especially troubleshooting security policies can be sometimes cumbersome and time consuming process. Here are some tips and possibilities how to perform it and what to look for.

Testing

Typically the most obvious way to test security policies is to issue traffic and check if it is being handled in the desired way. Following command can be used:

```
lab@srx1> show security flow session
```

The output lists the currently active sessions on the device. In addition the command offers rich filtering criteria (such as destination address, source address, both ports, protocol, incoming or outgoing interface, etc.) to aid in showing and checking only the desired sessions.

To generate such traffic an external device needs to be available and this might be sometimes hard to accomplish (no device available, security personnel has no access to it, etc.). In such cases the SRX devices offers a capability to test the security policies locally by using following command (available from the Junos release 10.3), e.g. the output of this command will show the details about the security policy handling the connection:

```
lab@srx1>show security match-policies ?
Possible completions:
  destination-ip       Match policy for the given destination IP
  destination-port     Match policy for the given destination port)
(1..65535)
  from-zone            Match policy for the given source zone
  protocol             Match policy for the given protocol)
  source-ip            Match policy for the given source IP
  source-port          Match policy for the given source port)
(1..65535)
  to-zone              Match policy for the given destination zone
```

NOTE: This command requires that ALL parameters are defined in order to be executed.

Another option for troubleshooting is enabling log action in security policies. The log entries contain information not only about the connection and its statistics but also the name of security policy handling the connection. In production environments with high traffic loads enabling security policies logging needs to be done with great caution as it can generate huge amount of log entries. This not

only consumes more system resources but might be harder to analyze due the amount of the log entries.

The tracing (or traceoptions) capability within Junos is intended to aid in troubleshooting in many areas including security policies. It provides detailed information about traffic processing and handling. The configuration is following:

```
[edit security flow]
lab@srx1# set traceoptions ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration
data
+ apply-groups-except   Don't inherit configuration data from these
groups
> file                  Trace file information
> flag                  Events and other information to include in
trace output
  no-remote-trace       Disable remote tracing
> packet-filter         Flow packet debug filters
  rate-limit            Limit the incoming rate of trace messages
(0..4294967295)
```

NOTE: When configuring the FLOW traceoptions always define the "**packet-filter**" with values that identify traffic you want to troubleshoot. This recommendation is crucial again in production environments by saving not only system resources but also speeding up the troubleshooting process as the traceoptions file will contain only entries related to processing of traffic matching the "packet-filter" criteria.

Some examples of common mistakes and causes of problems:

- Incorrect routing
  - the traffic crosses different zones than expected
  - the traffic for which forwarding lookup fails is dropped
- Security policies
  - wrong order of security policies
  - mistakes/typos in values of addresses (source, destination) and applications

Configurations

Below is the security policies related configuration for all lab devices:

Branch office 1

srx1 :

```
applications {
    application-set trust-app-set {
        application junos-http;
        application junos-https;
    }
}

security {
    zones {
        security-zone TRUST {
            address-book {
                address trust-address-range 172.16.10.0/24;
            }
            interfaces {
                ge-0/0/1.0;
            }
        }
        security-zone DMZ {
            address-book {
                address dmz-range 172.16.11.0/24;
            }
            interfaces {
                ge-0/0/2.0;
            }
        }
        security-zone UNTRUST {
            address-book {
                address corp-network 172.16.0.0/16;
            }
            interfaces {
                ge-0/0/3.0;
            }
        }
    }
    policies {
        from-zone TRUST to-zone UNTRUST {
     policy internet-access {
                match {
                    source-address trust-address-range;
                    destination-address any;
                    application trust-app-set;
                }
                then {
                    permit;
                }
            }
```

```
            policy corp-network-access {
                match {
                    source-address trust-address-range;
                    destination-address corp-network;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone TRUST to-zone DMZ {
            policy trust-to-dmz {
                match {
                    source-address trust-address-range;
                    destination-address dmz-range;
                    application junos-https;
                }
                then {
                    permit;
                }
            }
        }
        from-zone UNTRUST to-zone DMZ {
            policy corp-network-to-dmz {
                match {
                    source-address corp-network;
                    destination-address dmz-range;
                    application junos-https;
                }
                then {
                    permit;
                }
            }
        }
        from-zone DMZ to-zone UNTRUST {
            policy dmz-to-untrust-log {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    deny;
                    log {
                        session-init;
                    }
                }
            }
        }
    }
}
```

Branch office 2

srx2:

```
applications {
    application-set private-app-set {
        application junos-http;
        application junos-https;
        application junos-ssh;
        application junos-telnet;
        application junos-ftp;
    }
}

security {
    zones {
        security-zone TRUST {
            address-book {
                address trust-address-range 172.16.20.0/24;
            }
            interfaces {
                ge-0/0/2.0;
            }
        }
        security-zone PRIVATE {
            address-book {
                address private-range 172.168.21.0/24;
            }
            interfaces {
                ge-0/0/4.0;
            }
        }
        security-zone UNTRUST {
            address-book {
                address corp-network 172.16.0.0/16;
                address dmz-DC 172.16.150.0/24;
                address dmz-CO 172.16.55.0/24;
                address-set dmz-zones {
                    address dmz-CO;
                    address dmz-DC;
                }
            }
            interfaces {
                ge-0/0/3.0;
            }
        }
    }
    policies {
        from-zone TRUST to-zone UNTRUST {
            policy corp-network-access {
                match {
                    source-address trust-address-range;
                    destination-address corp-network;
                    application any;
```

```
                }
                then {
                    permit;
                }
            }
            policy internet-deny-log {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    deny;
                    log {
                        session-init;
                    }
                }
            }
        }
        from-zone TRUST to-zone PRIVATE {
            policy trust-to-private {
                match {
                    source-address trust-address-range;
                    destination-address private-range;
                    application junos-https;
                }
                then {
                    permit;
                }
            }
        }
        from-zone PRIVATE to-zone UNTRUST {
            policy dmz-access {
                match {
                    source-address private-range;
                    destination-address dmz-zones;
                    application private-app-set;
                }
                then {
                    permit;
                }
            }
        }
    }
}
```

Data center

cluster1:

```
applications {
    application custom-sql {
        application-protocol sqlnet-v2;
        protocol tcp;
```

```
            destination-port 5000-6000;
        }
        application-set dmz-apps {
            application junos-http;
            application junos-https;
            application junos-ssh;
            application junos-ftp;
            application junos-smtp;
            application junos-telnet;

        }
    }

    security {
        zones {
            security-zone TRUST {
                address-book {
                    address trust-address-range 172.16.100.0/24;
                }
                interfaces {
                    reth1.100;
                }
            }
            security-zone DMZ {
                address-book {
                    address dmz-range 172.16.150.0/24;
                }
                interfaces {
                    reth1.150;
                }
            }
            security-zone UNTRUST {
                address-book {
                    address corp-network 172.16.0.0/16;
                    address co-dmz-range 172.16.55.0/24;
                    address finance-range 172.16.199.0/24;
                }
                interfaces {
                    reth0.0;
                }
            }
            security-zone WAREHOUSE {
                address-book {
                    address warehouse-range 172.16.200.0/24;
                }
                interfaces {
                    reth1.200;
                }
            }
        }
    policies {
            from-zone TRUST to-zone UNTRUST {
                policy corp-access {
                    match {
                        source-address trust-address-range;
                        destination-address corp-network;
```

```
                application any;
            }
            then {
                permit;
            }
        }
        policy internet-denied-log {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                deny;
                log {
                    session-init;
                }
            }
        }
    }
    from-zone TRUST to-zone DMZ {
        policy trust-dmz-access {
            match {
                source-address trust-address-range;
                destination-address dmz-range;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone UNTRUST to-zone DMZ {
        policy access-from-corp {
            match {
                source-address corp-network;
                destination-address dmz-range;
                application dmz-apps;
            }
            then {
                permit;
            }
        }
    }
    from-zone TRUST to-zone WAREHOUSE {
        policy trust-warehouse-access {
            match {
                source-address trust-address-range;
                destination-address warehouse-range;
                application any;
            }
            then {
                permit;
            }
        }
    }
```

```
from-zone DMZ to-zone WAREHOUSE {
    policy dmz-warehouse-access {
        match {
            source-address dmz-range;
            destination-address warehouse-range;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone WAREHOUSE to-zone DMZ {
    policy warehouse-dmz-access {
        match {
            source-address warehouse-range;
            destination-address dmz-range;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone WAREHOUSE to-zone UNTRUST {
    policy warehouse-co-dmz-access {
        match {
            source-address warehouse-range;
            destination-address co-dmz-range;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone WAREHOUSE {
    policy co-dmz-warehouse {
        match {
            source-address co-dmz-range;
            destination-address warehouse-range;
            application any;
        }
        then {
            permit;
        }
    }
    policy finance-warehouse-access {
        match {
            source-address finance-range;
            destination-address warehouse-range;
            application custom-sql;
        }
        then {
            permit;
        }
```

```
            }
        }
    }
}
```

Central office

cluster2:

```
applications {
    application-set dmz-apps {
        application junos-http;
        application junos-https;
        application junos-ssh;
    }
    application-set dmz-apps-web-auth {
        application junos-ftp;
        application junos-telnet;
        application junos-http;
    }
    application-set internet-apps {
        application junos-http;
        application junos-https;
    }
}
schedulers {
    scheduler working-time {
        daily {
            start-time 08:00:00 stop-time 18:00:00;
        }
        sunday exclude;
        saturday exclude;
    }
}


security {
alg {
    dns {
        doctoring {
            sanity-check;    # <== task 23
        }
    }
}
    zones {
        security-zone TRUST {
            address-book {
                address trust-address-range 172.16.50.0/24;
            }
            interfaces {
                reth1.50;
            }
        }
security-zone DMZ {
```

```
            address-book {
                address dmz-range 172.16.55.0/24;
            }
            interfaces {
                reth1.55;
            }
        }
        security-zone INTERNAL {
            address-book {
                address internal-range 172.16.60.0/24;
                address finance-range 172.16.199.0/24;
                address private-range 172.16.21.0/24;
                address-set internal-finance-private-ranges {
                    address internal-range;
                    address finance-range;
                    address private-range;
                }
            }
            interfaces {
                reth1.60;
            }
        }
        security-zone UNTRUST {
            address-book {
                address corp-network 172.16.0.0/16;
                address dc-warehouse-range 172.16.200.0/24;
                address dc-dmz-range 172.16.150.0/24;
                address-set dc-dmz-warehouse {
                    address dc-dmz-range;
                    address dc-warehouse-range;
                }
            }
            interfaces {
                reth0.0;
            }
        }
    }
policies {
        from-zone INTERNAL to-zone UNTRUST {
            policy finance-dc-dmz-warehouse-access {
                match {
                    source-address finance-range;
                    destination-address dc-dmz-warehouse;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone INTERNAL to-zone DMZ {
            policy finance-dmz-access {
                match {
                    source-address finance-range;
                    destination-address dmz-range;
                    application any;
```

```
            }
            then {
                permit;
            }
        }
        policy internal-dmz-access {
            match {
                source-address internal-range;
                destination-address dmz-range;
                application any;
            }
            then {
                permit;
            }
            scheduler-name working-time;
        }
    }
    from-zone TRUST to-zone UNTRUST {
        policy trust-corp-network {
            match {
                source-address trust-address-range;
                destination-address corp-network;
                application any;
            }
            then {
                permit;
            }
        }
        policy internet-access {
            match {
                source-address trust-address-range;
                destination-address any;
                application internet-apps;
            }
            then {
                permit;
            }
        }
        policy internet-denied-log {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                deny;
                log {
                    session-init;
                }
            }
        }
    }
    from-zone TRUST to-zone DMZ {
        policy trust-dmz-access {
            match {
                source-address trust-address-range;
```

```
                    destination-address dmz-range;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone TRUST to-zone INTERNAL {
            policy trust-to-int-priv-fin {
                match {
                    source-address trust-address-range;
                    destination-address internal-finance-private-
ranges;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone DMZ to-zone UNTRUST {
            policy dmz-warehouse-access {
                match {
                    source-address dmz-range;
                    destination-address dc-warehouse-range;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone UNTRUST to-zone DMZ {
            policy warehouse-dmz-access {
                match {
                    source-address dc-warehouse-range;
                    destination-address dmz-range;
                    application any;
                }
                then {
                    permit;
                }
            }
            policy corp-dmz-acces-web-auth {
                match {
                    source-address corp-network;
                    destination-address dmz-range;
                    application dmz-apps-web-auth;
                }
                then {
                    permit {
                        firewall-authentication {
                            pass-through {
                                client-match testuser;
                            }
```

```
                        }
                    }
                }
            }
            policy corp-dmz-acces {
                match {
                    source-address corp-network;
                    destination-address dmz-range;
                    application dmz-apps;
                }
                then {
                    permit;
                }
            }
        }
    }
}
access {
    profile FWauth {
        authentication-order password;
        client testuser {
            firewall-user {
                password
"$9$Sm9yMXVb2aGiYgF/tpEhevWXdsYgJkmTJZn/tpB1"; ## SECRET-DATA
            }
        }
        session-options {
            client-idle-timeout 60;
        }
    }
    firewall-authentication {
        pass-through {
            default-profile FWauth;
            ftp {
                banner {
                    login "Look out firewall authentication!!!";
                    success "Correct!";
                    fail "Incorrect!";
                }
            }
            telnet {
                banner {
                    login "Look out firewall authentication!!!";
                    success "Correct!";
                    fail "Incorrect!";
                }
            }
        }
    }
}
```

Finance department

srx7:

```
applications {
    application custom-sql {
        application-protocol sqlnet-v2;
        protocol tcp;
        destination-port 5000-6000;
    }
    application-set dmz-apps {
        application junos-http;
        application junos-https;
        application junos-ssh;
    }
}


security {
    zones {
        security-zone FINANCE {
            address-book {
                address finance-address-range 172.16.199.0/24;
            }
            interfaces {
                ge-0/0/1.0;
            }
        }
        security-zone PRIVATE {
            address-book {
                address private-range 172.168.21.0/24;
            }
            interfaces {
                ge-0/0/2.0;
            }
        }
        security-zone INTERNAL {
            address-book {
                address dmz-DC 172.16.150.0/24;
                address dmz-CO 172.16.55.0/24;
                address warehouse-range 172.16.200.0/24;
                address internal-range 172.16.60.0/24;
                address-set dmz-zones {
                    address dmz-CO;
                    address dmz-DC;
                }
            }
            interfaces {
                ge-0/0/4.60;
            }
        }
    }
    policies {
        from-zone FINANCE to-zone INTERNAL {
            policy finance-internal {
                match {
                    source-address finance-address-range;
                    destination-address internal-range;
                    application any;
                }
```

```
                then {
                    permit;
                }
            }
            policy warehouse-sql {
                match {
                    source-address finance-address-range;
                    destination-address warehouse-range;
                    application custom-sql;
                }
                then {
                    permit;
                }
            }
            policy dmz-zone-access {
                match {
                    source-address finance-address-range;
                    destination-address dmz-zones;
                    application dmz-apps;
                }
                then {
                    permit;
                }
            }
        }
    }
}
```

Home office

srx8:

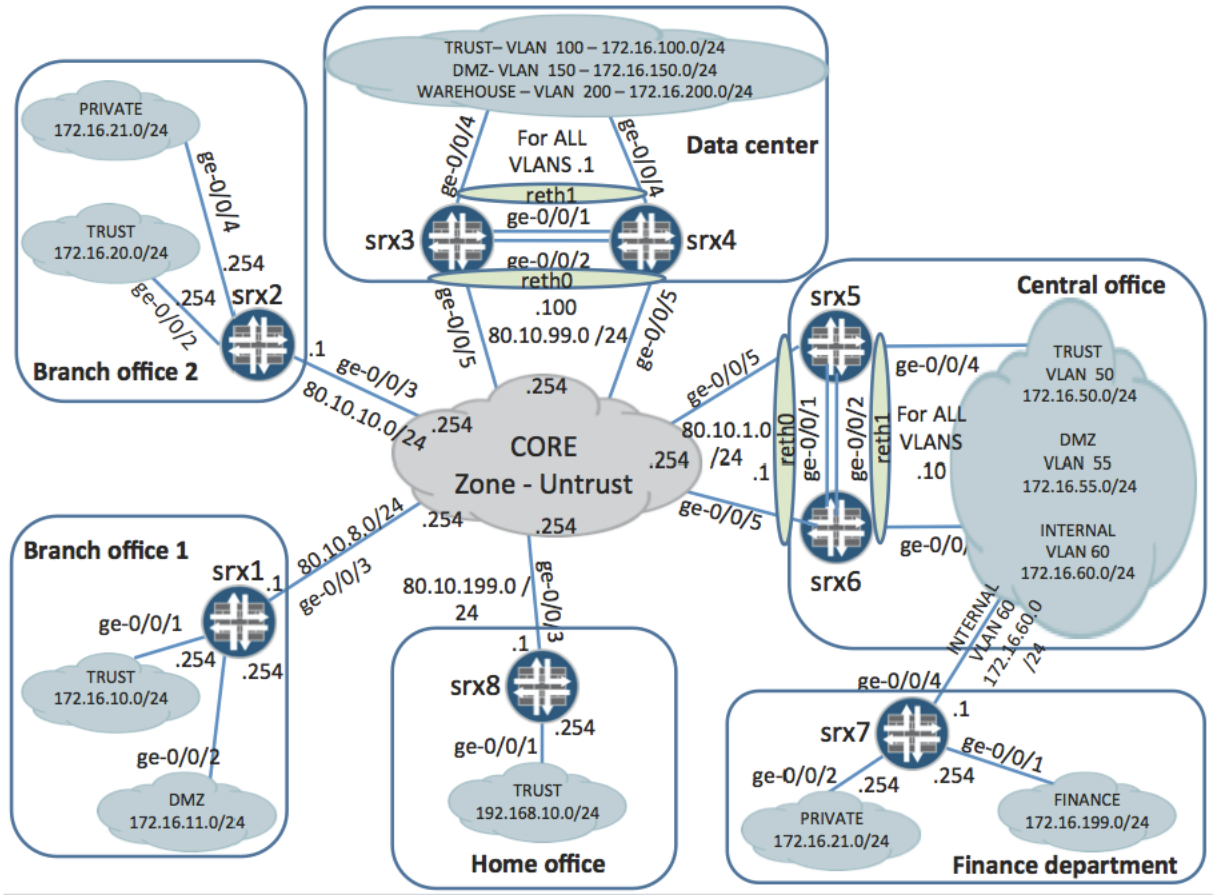
```
applications {
    application-set internet-apps {
        application junos-http;
        application junos-https;
    }
}


security {
    zones {
        security-zone TRUST {
            address-book {
                address trust-address-range 192.168.10.0/24;
            }
            interfaces {
                ge-0/0/1.0;
            }
        }
        security-zone UNTRUST {
            address-book {
                address corp-network 172.16.0.0/16;
            }
            interfaces {
```

```
                ge-0/0/3.0;
            }
        }
    }
    policies {
        from-zone TRUST to-zone UNTRUST {
            policy corp-network-access {
                match {
                    source-address trust-address-range;
                    destination-address corp-network;
                    application any;
                }
                then {
                    permit;
                }
            }
            policy internet-access {
                match {
                    source-address trust-address-range;
                    destination-address any;
                    application internet-apps;
                }
                then {
                    permit;
                }
            }
        }
    }
}
```

Appendix - Chapter four: Unified Threat Management

This appendix provides the solution details for the Unified Threat Management (UTM) chapter. The configuration involves web and content filtering, anti-spam and antivirus.

Topology for chapter four:



Task 1: Web-filtering

This part is dedicated to the web filtering.

The instructions define the existing policies should be reused whenever possible, e.g. associating the newly created utm-policy with already existing security policies.

The UTM configuration is located under the [edit security utm] stanza, but the associations of utm-policies and security policies are done in the security policies configuration under the "then permit" stanza.

Branch office: srx1

1) The following security policy created in the previous chapter can be used to enforce the web-filtering on the traffic from zone TRUST to UNTRUST.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx1	TRUST	UNTRUST	172.16.10.0/24	any	junos-http junos-https	permit

2) The web-filtering offers 3 options:
   a. surf-control-integrated
   b. websense-redirect
   c. juniper-local

   Following command defines that the surf-control type will be used for web-filtering, e.g.surf-control-integrated.

```
[edit security utm]
lab@srx1# set feature-profile web-filtering type surf-control-
integrated
```

   In the config examples the BranchOffice-Web was defined as the web-filtering feature profile name.

3) Using this method Junos security device consults the received http requests with defined SurfControl server. The security device makes the decision based on the returned URL's category. The configuration below assures the appropriate handling of requests according the requirements:
   d. Categories: Hacking, Violence, Gambling, Games --> blocked
   e. Categories: News, Computing_Internet --> permitted
   f. All other URL's --> permitted and logged
      i. The default action for URLs not matching any of the defined categories should be permit and log.

```
[edit security utm feature-profile web-filtering surf-control-
integrated profile BranchOffice-Web]
lab@srx1# show
```

```
category {
    Hacking {
        action block;
    }
    Violence {
        action block;
    }
    Gambling {
        action block;
    }
    Games {
        action block;
    }
    News {
        action permit;
    }
    Computing_Internet {
        action permit;
    }
}
default log-and-permit;
```

NOTE: The custom categories and URL's belonging to them are defined using custom objects under [edit security utm] stanza. The evaluation for custom categories precedes the predefined (SurfControl) ones.

4) Execute this command to define the custom message ("Blocked site!") clients will receive in case their request is blocked.

```
[edit security utm feature-profile web-filtering surf-control-
integrated profile BranchOffice-Web]
lab@srx1# set custom-block-message "Blocked site!"
```

5) The fallback options specify the engine behaviour when experiencing various issues when processing requests. The given instructions require following handling:
   g. For "too many requests" situation the action is drop/block

```
[edit security utm feature-profile web-filtering surf-control-
integrated profile BranchOffice-Web]
lab@srx1# set fallback-settings too-many-requests block
```

   h. Server communication problems (response timeout reached and lost connectivity) result in blocking the requests

```
[edit security utm feature-profile web-filtering surf-control-
integrated profile BranchOffice-Web]
lab@srx1# set fallback-settings server-connectivity block

[edit security utm feature-profile web-filtering surf-control-
integrated profile BranchOffice-Web]
lab@srx1# set fallback-settings timeout block
```

i. For all other causes (default) the action is permit and log

```
[edit security utm feature-profile web-filtering surf-control-
integrated profile BranchOffice-Web]
lab@srx1# set fallback-settings default log-and-permit
```

6) The following command defines 120 seconds as server communication timeout limit.

```
[edit security utm feature-profile web-filtering surf-control-
integrated profile BranchOffice-Web]
lab@srx1# set timeout 120
```

7) The configuration below shows the integrated SurfControl mode cache settings (size 1048576 B, timeout 30 minutes). The cache size is defined in bytes and the timeout in seconds.

NOTE: Although the Junos device allows definition of multiple integrated SurfControl profiles the cache and server connections details are defined only once (above the profile configuration hierarchy) and shared by all web-filtering profiles.

```
[edit security utm feature-profile web-filtering surf-control-
integrated]
lab@srx1# show
cache {
    timeout 1800;
    size 1m;
}
```

8) The SurfControl server connection details (IP 85.115.54.170, port 62252) are configured as follows:

```
[edit security utm feature-profile web-filtering surf-control-
integrated]
lab@srx1# show | find server
server {
    host 85.115.54.170;
    port 62252;
}
```

The remaining part is to define the utm policy (chosen name is "Branch-web-filter") referencing this created Branchoffice-Web web-filtering profile and then associate this utm policy with the correct security policy listed in the step 1.

```
[edit security utm]
lab@srx1# show | find utm-policy
utm-policy Branch-web-filter {
    web-filtering {
        http-profile BranchOffice-Web;
    }
}


[edit security policies from-zone TRUST to-zone UNTRUST]
lab@srx1# show
```

```
policy internet-access {
    match {
        source-address trust-address-range;
        destination-address any;
        application trust-app-set;
    }
    then {
        permit {
            application-services {
                utm-policy Branch-web-filter;
            }
        }
    }
}
```

Central office: cluster 2

9) The other available type (WebSense) of web-filtering has to be used on this device.

```
{primary:node0}[edit security utm]
lab@srx5# set feature-profile web-filtering type websense-redirect
```

10) It will be enabled on the following existing security policy between TRUST and UNTRUST zones.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	TRUST	UNTRUST	172.16.50.0/24	any	junos-http junos-https	permit

11) The URLs listed in the white-list are excluded from web-filtering. To satisfy the given requirements the use of wildcards is needed.

NOTE: Although the SRX allows using wildcards when defining URLs there are some limitations. The following wildcard rule applies: *\.[]\?* and you must precede all wildcard URLs with http://. You can only use "*" if it is at the beginning of the URL and is followed by a ".". You can only use "?" at the end of the URL. The following wildcard syntax is supported: http://*.juniper.net, http://www.juniper.ne?, http://www.juniper.n??. The following wildcard syntax is NOT supported: *.juniper.net , www.juniper.ne?, http://*juniper.net, http://*.

a. Bing.com site with the pages listing the search results should be permitted
    i. http://*.bing.com
b. The same applies for google.com
    ii. http://*.google.com
c. The juniper.net site is allowed
    iii. http://www.juniper.net

12) For denying defined URLs the black-list has to be used

d. Anything that start with www.facebook.com
    iv. http://www.facebook.com

```
{primary:node0}[edit security utm]
lab@srx5# show
```

```
custom-objects {
    url-pattern {
        Allowed-sites {
            value [ http://*.bing.com http://*.google.com
http://www.juniper.net ];
        }
        Blocked-sites {
            value http://www.facebook.com;
        }
    }
    custom-url-category {
        Allowed-sites-category {
            value Allowed-sites;
        }
        Blocked-sites-category {
            value Blocked-sites;
        }
    }
}
feature-profile {
    web-filtering {
        url-whitelist Allowed-sites-category;
        url-blacklist Blocked-sites-category;
    }
}
```

13) The configuration below shows the defined server details - IP address and port.

```
{primary:node0}[edit security utm feature-profile web-filtering
websense-redirect]
lab@srx5# show
profile central-Office-web-filtering {
    server {
        host 80.200.200.200;
        port 12345;
    }
}
```

14) The fallback settings define the request's handling when problems or issues arise, specifically the behaviour can be defined for following situations:

a. When the device cannot connect to the server
b. When the defined timeout for server responses elapses
c. When the engine received too many request
d. All other problems

Based on the instructions the actions for a. and b. are "block", and for c. and d. options are "permit and log".

```
{primary:node0}[edit security utm feature-profile web-filtering
websense-redirect profile central-Office-web-filtering]
lab@srx5# show | find fall
fallback-settings {
    default log-and-permit;
    server-connectivity block;
    timeout block;
```

```
    too-many-requests log-and-permit;
}
```

15) The command below sets the timeout for WebSense server responses to 180 seconds.

```
{primary:node0}[edit security utm feature-profile web-filtering
websense-redirect profile central-Office-web-filtering]
lab@srx5# set timeout 180
```

16) Definition of message the clients will receive in case of blocked request is:

```
{primary:node0}[edit security utm feature-profile web-filtering
websense-redirect profile central-Office-web-filtering]
lab@srx5# set custom-block-message "SRX blocked the request!"
```

17) The engine will include the string defined in the "account" parameter into the requests sent to WebSense to achieve specific treatment.

```
{primary:node0}[edit security utm feature-profile web-filtering
websense-redirect profile central-Office-web-filtering]
lab@srx5# set accountcentraloffice
```

18) The "sockets" pameters defines the limit for parallel connections to the WebSense server. It has to be set to 5 for the number of parallel connections to stay below 6.

```
{primary:node0} [edit security utm feature-profile web-filtering
websense-redirect profile central-Office-web-filtering]
lab@srx5# set sockets5
```

Similarly as on the srx1 device the utm-policy needs to be created and associated with appropriate security policy:

```
{primary:node0}[edit security utm]
lab@srx5# show | find utm-policy
utm-policy central-office-utm {
    web-filtering {
        http-profile central-Office-web-filtering;
    }
}

{primary:node0}[edit security policies from-zone TRUST to-zone
UNTRUST policy internet-access]
lab@srx5# show
match {
    source-address trust-address-range;
    destination-address any;
    application internet-apps;
}
then {
    permit {
        application-services {
            utm-policy central-office-utm;
        }
    }
```

```
}
```

Home office: srx8

19) The following security policy will be used to enforce the web-filtering:

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx8	TRUST	UNTRUST	192.168.10.0/24	any	junos-http junos-https	permit

20) The "juniper-local" option tells the device to make the web-filtering decisions purely on its own using white, black lists and default action.

```
[edit security utm feature-profile web-filtering]
lab@srx8# set type juniper-local
```

21) The same approach for configuring white and black lists as on the cluster 2 is used.

```
[edit security utm]
lab@srx8# set custom-objects url-pattern denied-sites value
http://www.facebook.com

[edit security utm]
lab@srx8# set custom-objects url-pattern denied-sites value
http://www.myspace.com

[edit security utm]
lab@srx8# set custom-objects custom-url-category denied-sites-
category value denied-sites
```

To deny these sites the created custom category has to be defined as black list.

```
[edit security utm feature-profile web-filtering]
lab@srx8# show
url-blacklist denied-sites-category;
```

22) The "default" action instructs the engine how it should handle all requests where the URL did not match the black or white list.

```
[edit security utm feature-profile web-filtering juniper-local
profile HomeOffice-web-filtering]
lab@srx8# set default permit
```

23) Following command defines the message the clients receive in case their request was blocked:

```
[edit security utm feature-profile web-filtering juniper-local
profile HomeOffice-web-filtering]
lab@srx8# set custom-block-message "This page is not allowed!"
```

24) This step requires all the fallback options to be set to block.

```
[edit security utm feature-profile web-filtering juniper-local
profile HomeOffice-web-filtering]
lab@srx8# show | find fallback
fallback-settings {
    default block;
    timeout block;
    too-many-requests block;
}
```

The remaining step is to create the utm-policy referencing the web-filtering profile and then associate the utm-policy with the appropriate security policy.

```
[edit security utm]
lab@srx8# show | find utm-policy
utm-policy home-office-utm {
    web-filtering {
        http-profile HomeOffice-web-filtering;
    }
}

[edit security policies from-zone TRUST to-zone UNTRUST policy
internet-access]
lab@srx8# show
match {
    source-address trust-address-range;
    destination-address any;
    application internet-apps;
}
then {
    permit {
        application-services {
            utm-policy home-office-utm;
        }
    }
}
```

Task 2: Antivirus

The information listed here is about the antivirus feature and its configuration based on the given requirements.

Home office: srx8

1) The full file-based scanning mode of operation for the antivirus engine is defined under "kaspersky-lab-engine"stanza in the anti-virus feature profile.
2) The configuration command below instructs the device to check for database updates automatically every 2 hours (120 minutes).
   The default URL is http://update.juniper-update.net/AV/<device version>, where the <device version> is the platform type, e.g. srx240, etc. Normally there is no need to change this default URL.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
lab@srx8# set pattern-update interval 120
```

3) The following existing security policy will be used, but in order to cope with the task the application-set needs to be adjusted by adding ftp and smtp applications to it. Because srx8 device already has the web-filtering enabled on this security policy, the existing utm-policy can be reused and only antivirus feature profile will be added to it the procedure is shown at the end of this task.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx8	TRUST	UNTRUST	192.168.10.0/24	any	junos-http junos-https	permit

```
[edit applications]
lab@srx8# show
application-set internet-apps {
    application junos-http;
    application junos-https;
    application junos-mail;
    application junos-ftp;
}

[edit security policies from-zone TRUST to-zone UNTRUST]
lab@srx8# show policy internet-access
match {
    source-address trust-address-range;
    destination-address any;
    application internet-apps;
}
then {
    permit {
        application-services {
            utm-policy home-office-utm;
        }
    }
}
```

4) Custom objects (url-pattern, custom-url-category) and "url-whitelist" parameter are used to exclude the prefix www.company.com from being scanned.

NOTE: The url-whitelist is defined for the whole anti-virus feature profile regardless of the engine mode of operation (full file-based, Juniper-Express, etc.)

```
[edit security utm]
lab@srx8# show custom-objects
url-pattern {
    company-site {
        value http://www.company.com;
    }
}
custom-url-category {
    AV-excluded-sites {
        value company-site;
    }
}

[edit security utm feature-profile anti-virus]
lab@srx8# show | match whitelist
url-whitelist AV-excluded-sites;
```

5) Similar approach is also valid for mime types - custom objects (mime-pattern) and "mime-whitelist" stanza. Prefixes need to be used for matching all video, application and audio mime types. The string used as prefix must have the "/" character placed at the end (for example "video/", "audio/", etc.)
Two mime patterns stanzas (list and exception) are available, one for excluding and one for including defined mime types from scanning respectively.

NOTE: The mime types are defined for the whole anti-virus feature profile regardless of the engine mode of operation (full file-based, Juniper-Express, etc.)

```
[edit security utm custom-objects]
lab@srx8# show mime-pattern
AV-excluded-mime {
    value [ audio/ video/ application/ ];
}
AV-included-mime {
    value [ application/javascript application/ecmascript ];
}


[edit security utm feature-profile anti-virus]
lab@srx8# show mime-whitelist
list AV-excluded-mime;
exception AV-included-mime;
```

6) The parameters under the "scan-options" stanza define the anti-virus engine behaviour. In order to fulfill the next couple of tasks these parameters need to be configured with appropriate values

Decompress limit set to 2 layers:

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine
profile AV-full-file-scan]
lab@srx8# set scan-options decompress-layer-limit 2
```

7) Scanning of all files regardless of file extension:

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine
profile AV-full-file-scan]
lab@srx8# set scan-options scan-mode all
```

8) Enabling the intelligent prescreening:

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine
profile AV-full-file-scan]
lab@srx8# set scan-options intelligent-prescreening
```

9) Scanning timeout set to 10 minutes (600 seconds)

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine
profile AV-full-file-scan]
lab@srx8# set scan-options timeout 600
```

10) The notifications details are configured under the "notification-options ", such as custom message text, notification type (message or protocol level error), if emails should be sent for email protocols (IMAP, POP3, SMTP). These parameters are defined separately for various situations:
    a. when virus is detected (step 34)
    b. when a problem occurs during processing the traffic and the engine blocks or permits the message (step 36)

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine
profile AV-full-file-scan notification-options]
lab@srx8# show
virus-detection {
    type message;
notify-mail-sender;
    custom-message "AV Engine detected virus!";
    custom-message-subject AntiVirus;
}
```

11) The "fallback-options" stanza contains parameters that define handling of packets for various cases, such as when the engine is out of resources, the scanning took too long, the engine is not ready, etc.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine
profile AV-full-file-scan]
lab@srx8# show fallback-options
default log-and-permit;
corrupt-file block;
password-file block;
decompress-layer block;
```

```
content-size block;
engine-not-ready block;
timeout block;
out-of-resources block;
too-many-requests block;
```

12) SRX allows defining notifications/messages for fallback situations. Messages and the notifications behavior are defined separately for cases when the action executed on the traffic is "block" and separately for the action "log-and-permit" (non-block). The configuration shown below defines the behavior as requested in this task.

NOTE: For NON-BLOCK cases the defined custom message is used only for email protocols. The other scanned protocols don't generate anything because the data is transmitted.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine
profile AV-full-file-scan]
lab@srx8# show notification-options | find fallback
fallback-block {
    type protocol-only;
    notify-mail-sender;
    custom-message  "AV denied the message, because it was not able
to scan it!"
    custom-message-subject AntiVirus;
}
fallback-non-block {
    notify-mail-recipient;
    custom-message "AV was not able to scan the message! ";
    custom-message-subject AntiVirus;
}
```

13) The antivirus scanning process takes time and sometimes can cause timeout on the clients receiving the data. The "trickling" feature can be used to prevent this situation. The engine sends periodically, in defined intervals, only small portions of the datato the recipient, even if the data has not been scanned yet.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine
profile AV-full-file-scan]
lab@srx8# set trickling timeout 25
```

As mentioned earlier the srx8 device has already utm-policy associated with appropriate security policy. Therefore the remaining task here is to modify the utm-policy and associate the created antivirus feature profile with the appropriate protocols (step 27 defines the http, ftp and smtp traffic is subject to scanning):

```
[edit security utm]
lab@srx8# show | find utm-policy
utm-policy home-office-utm {
    anti-virus {
        http-profile AV-full-file-scan;
        ftp {
            upload-profile AV-full-file-scan;
```

```
            download-profile AV-full-file-scan;
        }
        smtp-profile AV-full-file-scan;
    }
    web-filtering {
        http-profile HomeOffice-web-filtering;
    }
}
```

Task 3: Content filtering

This section provides details about the solution for the defined content filtering requirements.

Central office: cluster 2

1) Because the content filtering takes place on the traffic from zone TRUST to zone UNTRUST on the cluster 2, it is suitable to reuse the existing utm-policy (created in task 1).
2) New feature profile for content filtering covering following aspects needs to be defined:
    a. http content types: exe files, cookies and java applets
        i. The "block-content-type" stanza defines which content types in http messages are blocked

```
{primary:node0} [edit security utm feature-profile content-filtering
profile central-office-content-filter]
lab@srx5# show
block-content-type {
    java-applet;
exe;
http-cookie;
}
```

    b. mime: video prefix
        i. Similar as before the mime types have to be defined as custom objects and then referenced in the "block-mime" stanza. The use of prefixes is needed here to achieve matching all video mime types.

```
{primary:node0} [edit security utm]
lab@srx5# show custom-objects mime-pattern
mime-video-prefix {
    value video/;
}

{primary:node0} [edit security utm feature-profile content-filtering
profile central-office-content-filter]
lab@srx5# show
block-mime {
    list mime-video-prefix;
}
```

    c. bat and sh file extensions
        i. Also file extensions are defined as custom object and then referenced in the "block-extension" parameter.

```
{primary:node0} [edit security utm]
lab@srx5# show custom-objects filename-extension
blocked-file-ext {
    value [ bat sh ];
}

{primary:node0} [edit security utm feature-profile content-filtering
profile central-office-content-filter]
lab@srx5# show | match extension
block-extension blocked-file-ext;
```

d. http protocol TRACE

i. Here created custom object containing http command is referenced in the "protocol-command" statement.

```
{primary:node0} [edit security utm]
lab@srx5# show custom-objects protocol-command
http-TRACE {
    value trace;
}

{primary:node0} [edit security utm feature-profile content-filtering
profile central-office-content-filter]
lab@srx5# show | match match block-command
block-command http-TRACE;
```

3) Below is the custom message definition clients receive when the data is blocked.

```
{primary:node0} [edit security utm feature-profile content-filtering
profile central-office-content-filter]
lab@srx5# set notification-options custom-message "Blocked content
by SRX!"
```

Following parameter needs to be configured to tell the device to generate protocol error when blocking the data.

```
{primary:node0} [edit security utm feature-profile content-filtering
profile central-office-content-filter]
lab@srx5# set notification-options type protocol-only
```

4) The limit for parallel client connections and the action to be taken when the limit is reached are defined within the utm-policy itself in the "traffic-options" stanza.
Because the utm-policy exists and is already associated with correct security policy (task 1) the only remaining action is to define the newly created content blocking profile for it.

```
[edit security utm utm-policy central-office-utm]
lab@srx5# show
content-filtering {
    http-profile central-office-content-filter;
}
web-filtering {
    http-profile central-Office-web-filtering;
}
traffic-options {
    sessions-per-client {
        limit 15;
        over-limit block;
    }
}
```

Task 4: Antispam

The instructions to fulfill the antispam tasks are presented here.

Central office: cluster 2

1) The email server location is in DMZ zone and the IP address is 172.16.55.100.
2) Because the SMTP communication going to this server needs to be checked a new security policy has to be defined:
   a. zone context: UNTRUST --> to DMZ
   b. addresses: any --> 172.16.55.100
   c. application: junos-mail
   d. this policy needs to be placed before the existing ones to provide correct treatment for the smtp traffic going only to the mail server

```
[edit security]
lab@srx5# set zones security-zone DMZ address-book address smtp-
server 172.16.55.100/32


[edit security policies from-zone UNTRUST to-zone DMZ]
lab@srx5# show
policy SMTP-server {
    match {
        source-address any;
        destination-address smtp-server;
        application junos-mail;
    }
    then {
        permit;
    }
}
policy warehouse-dmz-access {
    match {
        source-address dc-warehouse-range;
        destination-address dmz-range;
        application any;
    }
    then {
        permit;
    }
}
…
```

3) The antispam feature is configured under the “edit security utm feature-profile anti-spam“ stanza. The white and black lists define in the antispam configuration allowed and denied sources (IP addresses, domains or email addresses) for email communication.
   The checking starts with evaluating the senders (or relay agents) IP address against the white list, and if no match is found the black list is examined for the IP address. If neither block nor white list resulted in a match the SBL (spam block list) server will be consulted, but only if it is explicitly configured. If the IP address did not result in any matches the domain is checked against the white list. Again if no match is found the domain is verified against the black list.

At last the email address of the sender is checked in similar manner as domain. If no match is found at all the email is normally transmitted.

NOTE: The antispam black and white list reference "url-pattern" custom object and NOT the "custom-url-category"!

The requirements define:

- 5.5.5.4 IP address is considered malicious --> black list
- 5.5.5.5 IP address is allowed --> white list
- 123.123.123.123 host is considered dangerous --> black list
- subject of the identified spam messages has to be tagged with the prefix "SPAM!!!"

4) The custom objects listed above needs to be modified to cover the requirements from this step.
   a. bad.com, spam.com --> black list
   b. spam@company.com, adv@company.com --> black list

```
[edit security utm custom-objects]
lab@srx5# show
url-pattern {
    allowed-mail-sources {
        value 5.5.5.5;
    }
    denied-mail-sources {
        value [ 5.5.5.4 123.123.123.123 bad.com spam.com
"spam@company.com" "adv@company.com" ];
    }
}

[edit security utm feature-profile anti-spam]
lab@srx5# show
address-whitelist allowed-mail-sources;
address-blacklist denied-mail-sources;
sbl {
    profile SMTP-server-antispam-prof {
        spam-action tag-subject;
        custom-tag-string "SPAM!!!";
    }
}
```

5) To tell the device to perform the decisions internally without consulting the SBL server following statement has to be executed:

```
[edit security utm feature-profile anti-spam]
lab@srx5# set sbl profile SMTP-server-antispam-prof no-sbl-default-
server
```

Again as in the previous tasks the utm-policy needs to created and associated with appropriate security policy.

```
[edit security utm utm-policy SMTP-server-utm-policy]
```

```
lab@srx5# show
anti-spam {
    smtp-profile SMTP-server-antispam-prof;
}

[edit security policies from-zone UNTRUST to-zone DMZ policy SMTP-
server]
lab@srx5# show
match {
    source-address any;
    destination-address smtp-server;
    application junos-mail;
}
then {
    permit {
        application-services {
            utm-policy SMTP-server-utm-policy;
        }
    }
}
```

Task 5: Testing

The SRX device provides a simple tool (operational mode command) for checking the utm configuration (anti-spam, anti-virus, web-filtering).

```
lab@srx5> test security utm ?
Possible completions:
  anti-spam            Test anti-spam profile
  anti-virus           Test anti-virus profile
  web-filtering        Test web-filtering profile
```

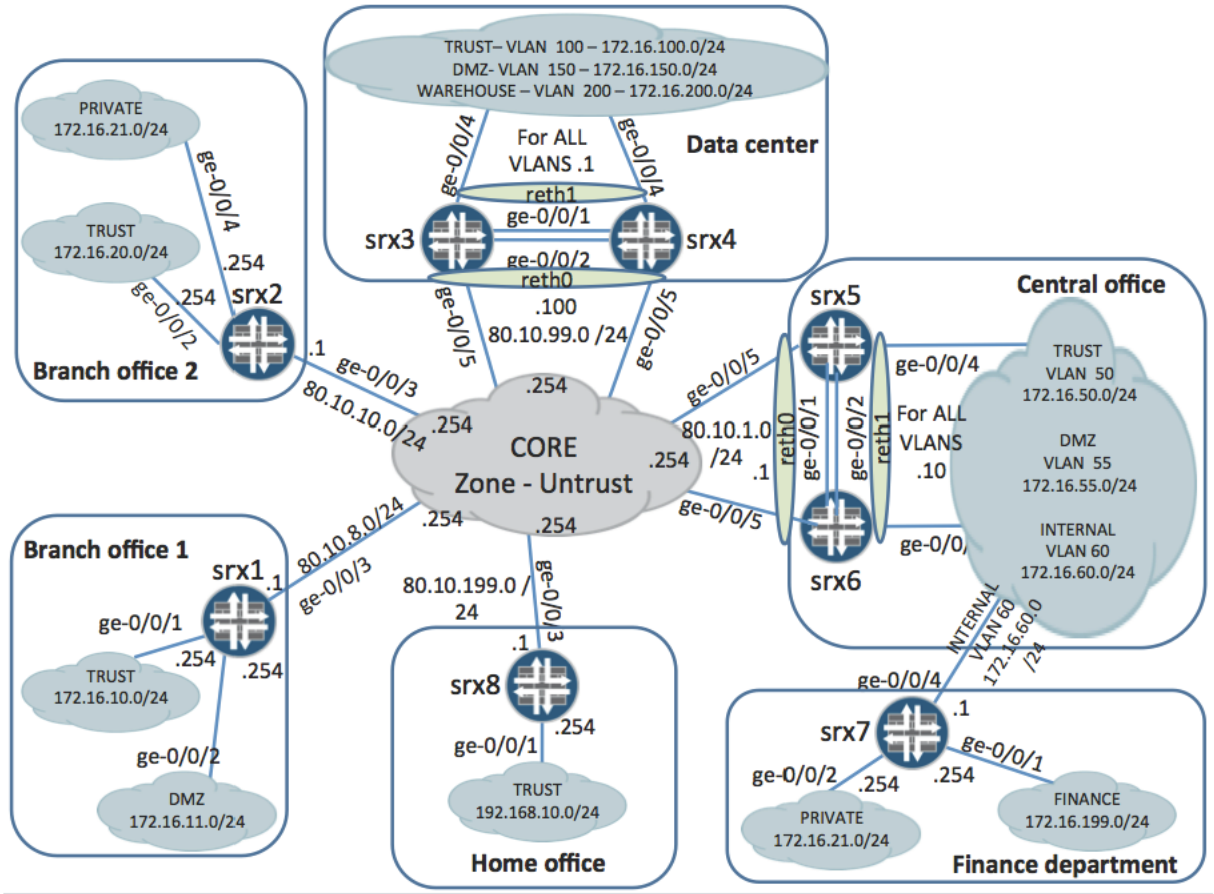
Example:

```
lab@srx5> test security utm anti-spam profile SMTP-server-antispam-
prof test-string 123.123.123.123
Anti-spam test result:
Return SPAM, action Tag email subject, reason Match local blacklist

lab@srx5> test security utm anti-spam profile SMTP-server-antispam-
prof test-string 5.5.5.5
Anti-spam test result:
Return NON SPAM, action Pass, reason Match local whitelist
```

Appendix - Chapter five: IPSec VPNs

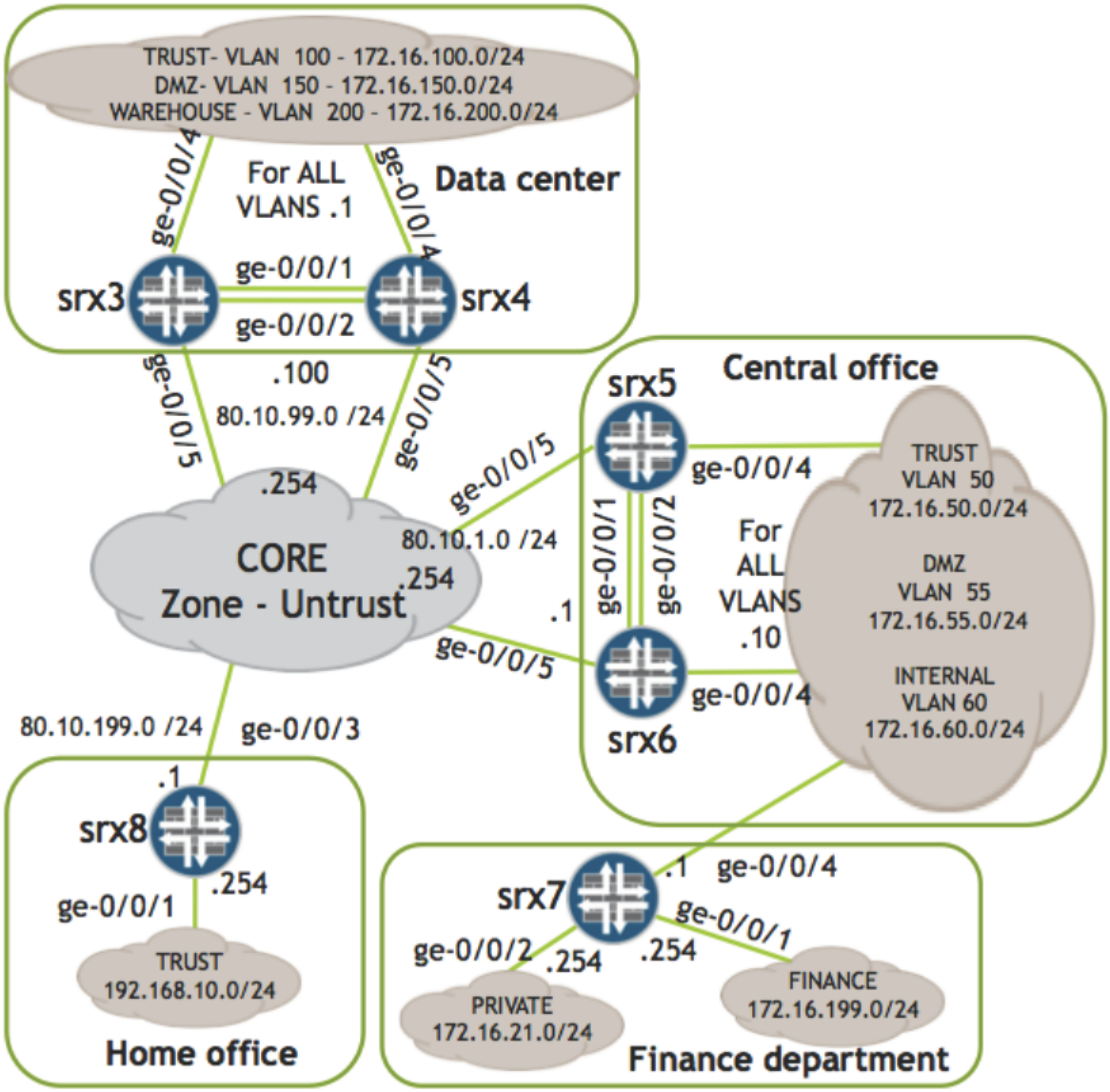
The purpose of this appendix is to guide you through the milestones of Chapter 5. You will find here configuration excerpts, tips and recommendations for successful completion of IPSec VPN tasks.

Topology for chapter five:



Task 1: Configuring Policy-based VPN

Task 1 Topology.



In this part you will configure lab equipment as necessary to build Policy-based VPN between Data Center, Home Office and Finance department.

1) Configure the IPSec VPN on every device according to the table below, which reflects the topology image.

Local Peer	Interface	Security zone	Remote Peer	Interface	Security zone
srx7	ge-0/0/4.60	Untrust	Cluster1	reth0.0	Untrust
srx8	ge-0/0/3.0	Untrust	Cluster1	reth0.0	Untrust

NOTE: Chapter 3 states the loopback association to security zones is free unless explicitly defined by a task. In case the loopback interfaces should be used as IPsec VPN termination points keep in mind they have to be associated with the same zone as the physical external

interfaces (KB22129). I.e. the KB22129 describes that the VPN setup where the loopback and physical external interface are located in different security zones is not supported.

At this step it would be a good idea to verify that operational configuration is available in security devices. The commands below can be used for that verification:

```
lab@srx8>show interface ge-0/0/3.0 terse
```

Ensure that the IKE traffic destined to the ge-0/0/3.0 interface is accepted by security zone settings.

```
lab@srx8>show security zone security-zone Untrust
```

Ensure that security policy allows intrazone traffic for Untrust security zone.

```
lab@srx8>show security policy from-zone Untrust to-zone Untrust
```

2) Central Office srx5/srx6 cluster provides only dynamical NAT-src service.
Use "load merge relative" command to insert interface-based NAT configuration into the cluster2. Configuration file is already copied to user's directory and has a name "int-based-nat-cluster2-c5t1".

```
[edit security nat]
source {
   rule-set int-nat {
        from zone INTERNAL;
        to zone UNTRUST;
        rule for-finance-dep {
             match {
                  source-address 172.16.60.0/24;
             }
             then {
                  source-nat interface;
}
        }
    }
}
```

3) VPN between srx8 and Cluster1 must meet the following requirements:

Configuration for the steps a) and b) below can be done from the `[edit security ike]` level of CLI hierarchy. There are three configuration elements that need to be defined there: Phase1 IKE proposal, Phase1 IKE policy and Phase1 IKE gateway.

a. Validate peer reachability with DPD option. The keepalives should be sent to the neighboring peer regardless of traffic patterns every 10 seconds. Consider peer unreachable if the number of DPD retransmissions exceeds 5 packets.
b. IKE phase 1 proposal must include: preshared key "juniper", DES, DH G1, MD5. Rekey Phase1 every 24 hours.

```
[edit security ike proposal ike-proposal]
```

```
authentication-method pre-shared-keys;
dh-group group1;
authentication-algorithm md5;
encryption-algorithm des-cbc;
lifetime-seconds 86400;
```

NOTE: The proposal must be the same for both peers that are participating in Phase1 establishment. The mistake at this configuration step will lead to the failure of Phase1 establishment with the possible cause code "`No proposal chosen`" in the kmd log on the responder's side.

The preshared key's value together with the tunnel's mode is defined in the Phase1 IKE Policy. The previously defined Phase1 proposal also referenced in the Phase1 policy:

```
[edit security ike policy ike-policy]
mode main;
proposals ike-proposal;
pre-shared-key ascii-text "$9$/Xo/Au17-wRh-wYgUD9Ap"; ## SECRET-DATA
```

NOTE: The other possible issue during Phase1 configuration is a mismatch of preshared key's value. The mistake at this configuration step will lead to the failure of Phase1 establishment with the possible cause code "`Invalid payload type`" in the kmd log on the responder's side.

Final step of Phase1 configuration is a gateway definition.

```
[edit security ike gateway ike-gateway]
ike-policy ike-policy;
address 192.168.2.1;
dead-peer-detection {
   always-send;
   interval 10;
   threshold 5;
}
external-interface ge-0/0/3.0;
```

NOTE: One more possible issue during Phase1 configuration is a mismatch of peers' logical interfaces that are specified with the "`address`" and "`external-interface`" keywords. The mistake at this configuration step will lead to the failure of Phase1 establishment with the possible cause code "`Remote peer is not recognized`" in the kmd log on the responder's side.

Configuration for steps c) can be done from the `[edit security ipsec]` level of CLI hierarchy.

c. IKE phase 2 proposal must include: AES128, ESP, DH G2, SHA1. Rekey Phase2 every 12 hours.

The configuration excerpts below provides you with the idea how IPSec part of configuration should look like.

```
[edit security ipsec proposal ipsec-proposal]
protocol esp;
authentication-algorithm hmac-sha1-96;
encryption-algorithm aes-128-cbc;
lifetime-seconds 43200;
```

NOTE: The proposal must be the same for both peers that are participating in IPSec tunnel establishment. The mistake at this configuration step will lead to the failure of Phase2 establishment with the possible cause code "`No proposal chosen`" in the kmd log on the responder's side.

The Perfect Forward Secrecy must be configured according to conditions of task c). You can accomplish it by specifying DH group at appropriate part of IPSec policy's configuration.

```
[edit security ipsec policy ipsec-policy]
perfect-forward-secrecy {
    keys group2;
}
proposals ipsec-proposal;
```

Next step is to bind together previously configured IKE gateway and IPSec policy, so Phase1 and Phase2 parameters will be combined together and associated with the IPSec VPN's name. One more thing to do is to specify conditions for tunnel establishment with the key word "`establish-tunnels`", which can be either immediately upon commit (value " immediately") or when traffic for the VPN arrives (value "on-traffic"). Because the task does not explicitly define the value, configure the value "immediately" to test whether the VPN configuration is correct.

```
[edit security ipsec vpn to-cluster1]
ike {
     gateway ike-gateway;
     ipsec-policy ipsec-policy;
}
establish-tunnels immediately;
```

d. Ensure that any traffic originated from TRUST zone of Home Office can reach only TRUST zone located in the Data Center and vice versa.

There are two ways to direct traffic into the IPSec tunnel:

1) The security policies define which traffic must forwarded via the tunnel;
2) The routing table directs traffic destined to the particular prefixes via the tunnel.

This task is dedicated for policy-based vpns and you need to create such a security policies that will allow to accomplish step d) conditions.

The configuration excerpts below is representing srx8 settings, although cluster1 configuration is similar.

There are two paired policies that describe traffic between TRUST zones of the Home office and the Data Center. Since this configuration is added to the existing one, you should make sure that the old policies in the same zone context do not shade new policies. Use command "`insert`" to move the new policy above the old one if it is necessary.

```
[edit security policies from-zone TRUST to-zone UNTRUST]
policy ipsec-out {
    match {
        source-address trust-address-range;
        destination-address dc-trust-address-range;
        application any;
    }
    then {
        permit {
            tunnel {
                ipsec-vpn to-cluster1;
                pair-policy ipsec-in;
            }
        }
    }
}

[edit security policies from-zone UNTRUST to-zone TRUST]
policy ipsec-in {
    match {
        source-address dc-trust-address-range;
        destination-address trust-address-range;
        application any;
    }
    then {
        permit {
            tunnel {
                ipsec-vpn to-cluster1;
                pair-policy ipsec-out;
            }
        }
    }
}
```

NOTE: Keep in mind that ProxyID values for Phase2 negotiation are derived from the security policies. If address book entries referenced as the source-address on one end of the tunnel and the destination-address on the other end of the tunnel are not match it will lead to the failure of Phase2 establishment with the possible cause code "`Failed to match the peer proxy ids`".

e. Collect the IKE Phase2 security association's management events in the kmd file on the cluster1.

```
[edit security ipsec]
traceoptions {
    flag security-associations;
```

```
}
```

If you were careful enough, you noticed that the proposed sequence of configuration actions for steps c) e) is not optimal. You configured IPSec parameters, after that you switched to the security policies configuration and, finally, you returned back to the IPSec traceoptions.

This implies a simple conclusion that preliminary study of all the tasks can help you making more efficient use of your time.

TIP: Ensure you read the entire chapter, before starting with the first task.

4) VPN between srx7 and Cluster1 must meet following requirements:
   a. Validate peer reachability with DPD option. The keepalives should be sent to the neighboring peer regardless of traffic patterns every 10 seconds. Consider peer unreachable if the number of DPD retransmissions exceeds 5 packets.
   b. IKE phase 1 proposal must include: preshared key "inetzero", 3DES, DH G5, SHA1. Rekey Phase1 every 24 hours.

The main difference between this step and step 4) is the Phase1 configuration.

The connection between srx8 and cluster1 is established using statically assigned IP addresses. So, the Phase1 mode configured for srx8 and cluster1 is Main mode.

The connection between srx7 and cluster1 is established using dynamically assigned IP address on the srx7 side. That is why the Phase1 mode must be configured as Aggressive mode in IKE policy.

```
[edit security ike policy ike-policy]
lab@srx7# show
mode aggressive;
```

One more setting that need to be done on the initiator's side is the local-identity value. Example below uses local-identity's type "hostname" and value "srx7".

```
[edit security ike gateway ike-gateway]
lab@srx7# show
local-identity hostname srx7;
```

Same string "srx7" must be configured on the responder's side as dynamic hostname's value.

```
[edit security ike gateway ike-gateway]
lab@cluster1# show
dynamic hostname srx7;
```

   c. IKE phase 2 proposal must include: AES-192, ESP, and SHA1. Rekey IPSec tunnel on transmitting 5 MB of traffic.

The IPSec tunnel's lifetime can be described either as period of time or amount of traffic forward through the tunnel. The example below shows how to accomplish conditions of step c).

```
[edit]
lab@srx7#set security ipsec proposal ipsec-proposal lifetime-
kilobytes 5000;
```

   d. Ensure that only traffic originated from the FINANCE zone of srx7 can reach Warehouse zone located in the Data Center and vice versa. This traffic must trigger the tunnel establishment.

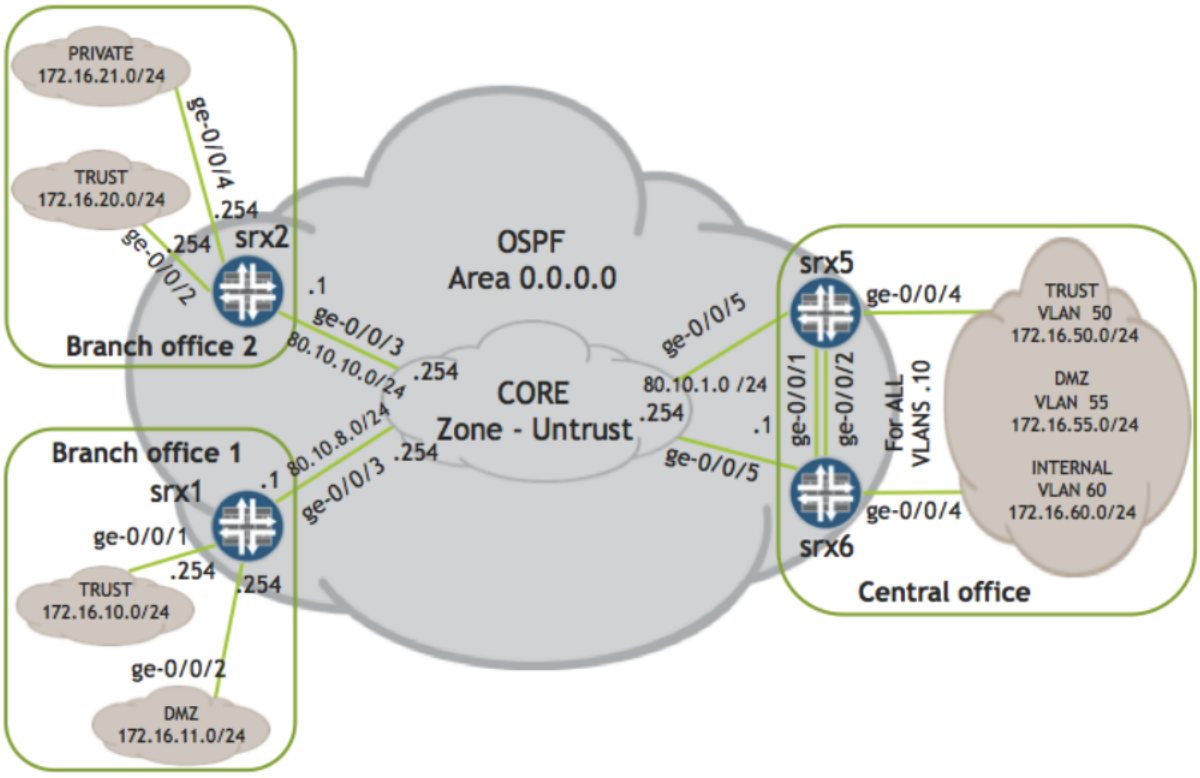
As mentioned before the "`establish-tunnels`" parameter controls that. Here the task explicitly requires the "on-traffic" value. To test if the configuration is correct and such IPsec VPN tunnel established a traffic needs to be received on the firewall that matches the security policy referencing the VPN, i.e. when generating traffic to start the VPN make sure the source and destination IP addresses match the security policy that has the VPN name defined in the action.

Another option is to define the "immediately" value for the "`establish-tunnels`" parameter to make the IPsec VPN to start upon commit. If the configuration is validated by the IPsec VPN coming up correctly change the "`establish-tunnels`" parameter value back to "on-traffic" to comply with the task.

e. Collect the IKE Phase2 security association's management events in the kmd file on the cluster1.

Task 2: Configuring Route-based VPN

Task 2 Topology.



In this part you will configure lab equipment as necessary to build full meshed Route-based VPN between Central Office, Branch office 1 and Branch office 2.

1) Branch offices have direct tunnel to each other and can communicate either directly or via Data Center. The forwarding decision is done on the base of tunnel's state.

Configure the interfaces on every device according to the table below, which reflects the topology image.

Device	Interface	IP address	VLAN-ID	Zone
srx1	st0.0	11.0.0.2/30	None	Untrust
srx1	st0.1	11.0.0.10/30	None	Untrust
srx2	st0.0	11.0.0.6/30	None	Untrust
srx2	st0.1	11.0.0.9/30	None	Untrust
Cluster2 (srx5, srx6)	st0.0	11.0.0.1/30	None	Untrust
Cluster2 (srx5, srx6)	st0.1	11.0.0.5/30	None	Untrust

The configuration that you need to create at this step is similar to task 1 of chapter 3 "Firewall Security Policies". Below is the configuration excerpt for tunnel interfaces of srx1.

```
[edit interfaces]
st0 {
    unit 0 {
        family inet {
            address 11.0.0.2/30;
        }
    }
    unit 1 {
        family inet {
            address 11.0.0.10/30;
        }
    }
}
```

At this step you also need to add st0 interfaces to the UNTRUST zone and verify that OSPF is the protocol permitted by host-inbound-traffic.

```
[edit security zones security-zone UNTRUST]
host-inbound-traffic {
    protocols {
        ospf;
    }
}
interfaces {
    ge-0/0/3.0;
    lo0.0;
    st0.0;
    st0.1;
}
```

Configure the IPSec VPN on every device according to the table below, which reflects the topology image.

Local Peer	Interface	Remote Peer	Interface
Cluster2	reth0.0	srx1	ge-0/0/3.0
Cluster2	reth0.0	srx2	ge-0/0/3.0
srx1	ge-0/0/3.0	srx2	ge-0/0/3.0

2) In this task's topology you will use OSPF as a dynamic routing protocol.
The subnets located in TRUST, PRIVATE, INTERNAL or DMZ zones must appear as OSPF internal routes on all devices in OSPF area 0, but no IGP adjacencies may be formed across interfaces located within these security zones.

Ensure that traffic originated from any TRUST zone can reach any other TRUST zone.

To accomplish this requirement you should create two security policies that describe traffic between TRUST zones of the Branch office 1, Branch office 2 and the Central office. Since this configuration is added to the existing one, you should make sure that the old policies in the same zone context do not shade new policies. Use command "`insert`" to move the new policy above the old one if it is necessary.

Configure the interfaces on every device according to the table below, which reflects the topology image.

Device	Interface	OSPF Area
srx1	st0.0	OSPF Area 0
srx1	st0.1	OSPF Area 0
srx1	ge-0/0/1.0	OSPF Area 0
srx1	ge-0/0/2.0	OSPF Area 0
srx2	st0.0	OSPF Area 0
srx2	st0.1	OSPF Area 0
srx2	ge-0/0/2.0	OSPF Area 0
srx2	ge-0/0/4.0	OSPF Area 0
Cluster2 (srx5, srx6)	st0.0	OSPF Area 0
Cluster2 (srx5, srx6)	st0.1	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.50	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.55	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.60	OSPF Area 0

To accomplish the whole task you need to create OSPF area 0.0.0.0 and place all appropriate interfaces in this area. The interfaces that are associated with TRUST, PRIVATE, INTERNAL or DMZ zones should be configured as passive. Below is the configuration excerpt for OSPF protocol configuration.

```
[edit protocols ospf area 0.0.0.0]
lab@srx1#show
interface st0.0;
interface st1.0;
interface ge-0/0/1.0 {
    passive;
}
interface ge-0/0/2.0 {
    passive;
}
```

3) VPN between srx1 and Cluster2 and between srx2 and Cluster2 must meet following requirements:
   a. Rekey IPSec tunnel every 8 hours;
   b. Validate data path with VPN monitor option. The keepalives should be sent to the neighboring peer regardless of traffic patterns with 5 sec interval. It is allowed to miss only three consecutive keepalives after which the tunnel is considered inactive.
   c. IKE phase 1 proposal must include: preshared key "inetzero", AES128, DH G2, SHA.
   d. IKE phase 2 proposal must include: AES256, ESP, SHA.
   e. Ensure that in case of one tunnel's failure traffic originated from the TRUST security zone of any site still can reach other site's protected recourses.
4) VPN between srx1 and srx2 must meet following requirements:
   a. Rekey IPSec tunnel on transmitting 100 MB of traffic;
   b. Validate data path with VPN monitor option. The keepalives should be sent to the neighboring peer only in absence of traffic patterns.
   c. IKE phase 1 proposal must include: preshared key "inetzero", 3DES, DH G2, MD5.
   d. IKE phase 2 proposal must include: AES256, ESP, SHA.
   e. Ensure that in case of one tunnel's failure traffic originated from the TRUST security zone of any site still can reach other site's protected recourses.

The main differences between IKE / IPSec configurations for Task 1 and Task 2 are:

1) The way traffic is forwarded into the IPSec tunnel. Task 2 assumes that security devices use routing tables' information instead of security policies.
   This is accomplished by enabling dynamic routing protocol on srx1, srx2 and cluster2. The OSPF learns prefixes reachability and maintain routing information into the inet.0 routing table.
   The one more mandatory configuration step that you need to do is the binding of tunnel interfaces to the IPSec VPN. Below is the command you can use for this task.

```
[edit]
lab@srx1#set security ipsec vpn to-cluster2bind-interface st0.0;
```

2) The replacement of DPD feature with the VPN monitor.
   This task requires you to monitor IPSec tunnel state with the VPN monitor feature that is available at the `[edit security ipsec]` level of configuration hierarchy.
   The "`optimized`" keyword allows using traffic patterns as an evidence of peer's aliveness.

```
[edit security ipsec vpn to-cluster2]
vpn-monitor {
    optimized;
    source-interface lo0.0;
    destination-ip 192.168.1.1;
}
```

The interval and threshold for VPN monitor keepalives can be configured at `[edit security ipsec vpn-monitor-options]` the level of configuration hierarchy.

```
[edit security ipsec vpn-monitor-options]
```

```
interval 5;
threshold 3;
```

Task 3: Configuring GRE-tunnel over Route-based VPN

Task 3 Topology.

In this part you will configure lab equipment as necessary to build GRE-tunnel over Route-based VPN between Branch Office 1 and Branch Office 2.

1) Configure the interfaces on every device according to the table below.
   The GRE tunnel source should be configured as device's local lo0 interface address and the destination should be configured as remote device's lo0 interface address.

Device	Interface	IP address	VLAN-ID	Zone
srx1	gr-0/0/0.0	11.11.11.1/30	None	Untrust
srx1	lo0.0	192.168.1.1/32	None	Untrust
srx2	gr-0/0/0.0	11.11.11.2/30	None	Untrust
srx2	lo0.0	192.168.1.2/32	None	Untrust

TIP: Ensure that GRE tunnel's termination points are reachable via the IPSec tunnel

The configuration that you need to create at this step is similar to task 1 of chapter 3 "Firewall Security Policies". Below is the configuration excerpt for GRE interfaces of srx1.

```
[edit interfaces gr-0/0/0]
unit 0 {
    tunnel {
        source 192.168.1.1;
        destination 192.168.1.2;
    }
    family inet {
        address 11.11.11.1/30;
    }
}
```

2) You need to configure OSPF as a dynamic routing protocol running between Branch Office 1 and Branch Office 2.
   Configure the interfaces on every device according to the table below, which reflects the topology image.

Device	Interface	OSPF Area
srx1	gr-0/0/0.0	OSPF Area 0
srx2	gr-0/0/0.0	OSPF Area 0

3) Ensure that any traffic originated from TRUST zone of Branch Office 1 can reach TRUST zone of the Branch Office 2 and vice versa.

Task 4: Configuring Dynamic VPN

In this part you need to configure remote access to the Data Center's protected resources located in the WAREHOUSE security zone. Configure remote access via IPSec VPN for the client's machine located in the CORE network in such way that it satisfy following requirements.

1) The initial client's connection can be done only via https on the IP address 80.10.99.100.

At this step, it is just a right time to check if https protocol is enabled both at `[edit system services web-management]` and at `[edit security zone security-zone UNTRUST host-inbound traffic]` levels of configuration hierarchy.

2) User must be authenticated with following settings:
   a. Username: testuser, password: testuserpw123
   b. Reauthentication after 1 hour of inactivity
   c. Local authentication
   d. Banners:
      v. In case of successful authentication: "Correct!"

To configure the security device to perform a firewall Web authentication the following steps need to be done:

- An access profile needs to be defined. In our case, access profile `FWauth` has been already created in chapter 3. You can speed up the configuration process by copy/paste this piece of configuration from cluster2 to cluster1. The only difference with the cluster2 configuration is the reference to pool of IP addresses that should be allocated to dynamic IPSec VPNs.

```
[edit]
access {
    profile FWauth {
        authentication-order password;
        client testuser {
            firewall-user {
                password
"$9$Sm9yMXVb2aGiYgF/tpEhevWXdsYgJkmTJZn/tpB1"; ## SECRET-DATA
            }
        }
        session-options {
            client-idle-timeout 60;
        }
        address-assignment {
             pool warehouse-pool;
        }
    }
```

- Firewall Web authentication setting need to be done:
  - Banners
  - Which access profile to use

```
[edit access]
firewall-authentication {
    web-authentication {
```

```
default-profile FWauth;
banner {
success "Correct!";
}
```

3) The IP address allocated to client's IPSec tunnel must be borrowed from the range of IP addresses 172.16.200.150 172.16.200.159.

Below is the configuration excerpt for the pool of IP addresses.

```
[edit access address-assignment]
pool warehouse-pool {
    family inet {
        network 172.16.200.0/24
        range remote-clients [
            low 172.16.200.150;
            high 172.16.200.159;
        }
    }
}
```

As soon as the range of IP addresses is borrowed from the network directly connected to the security device you need to enable Proxy ARP on the appropriate interface.

4) Use predefined proposals "Basic" for IKE Phase1 and Phase2.

The dynamic IPSec tunnel configuration is similar to configuration of previously discussed scenarios. The specialties of dynamic IPSec VPN are:

- It works only in aggressive mode;
- Only preshared keys can be used during Phase1 authentication;
- The XAUTH needs to be configured for IKE Phase1 gateway. This authentication mechanism uses same database as the Web authentication uses.

5) Ensure that client has access to the Data Center network 172.16.200.0/24 via the IPSec tunnel. The traffic destine to other prefixes must bypass IPSec tunnel.

As soon as all IKE/IPSec parameters are defined you can configure dynamic vpn itself. The configuration is done from the `[security dynamic-vpn]` level of configuration hierarchy. It includes binding together previously defined access-profile and ipsec vpn.

Furthermore, dynamic vpn's configuration defines list of users that can establish tunnels and the network prefixes that must be reachable via the vpn. Below is the configuration excerpt illustrating this configuration step.

```
[edit security dynamic-vpn]
access-profile FWauth;
clients [
    all [
        remote-protected-resources {
            172.16.200.0/24;
        }
        remote-exceptions {
            0.0.0.0/0;
```

```
        }
        ipsec-vpn dynamic-vpn-to-warehouse;
        user {
testuser;
        }
```

Finally, IPSec VPN "dynamic-vpn-to-warehouse" need to be anchored to the security policy that defines client's traffic from the UNTRUST zone to WAREHOUSE zone.

```
[edit security]
policy dyn-vpn-policy {
    match {
        source-address any;
        destination-address warehouse-range;
        application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn dynamic-vpn-to-warehouse;
                    }
                }
            }
         }
```

Task 5: Verification

IKE Phase 1 operations can be verified with following command:

1) The `show security ike` command provides you with the variety of possible completions. It allows you delve furthermore into device's operations and, possible find clear answers to your concerns.
   a. The "`active-peer`" completion is useful if you want to verify how DPD works.

```
lab@srx8> show security ike active-peer
Remote Address    Port      Peer IKE-ID      XAUTH username     Assigned IP
192.168.2.1       500       192.168.2.1
```

   b. Next option can be used either in brief or in detailed format depending your needs for information. This command is a good way to verify that Phase1 is successfully completed.

```
lab@srx8> show security ike security-associations
 Index     Remote Address  State   Initiator cookie  Responder cookie  Mode
 7147529   192.168.2.1     UP      25a11b0b6aa11f5d  79dceeea95d85718  Main

lab@srx8> show security ike security-associations detail
IKE peer 192.168.2.1, Index 7147529,
  Role: Initiator, State: UP
  Initiator cookie: 25a11b0b6aa11f5d, Responder cookie: 79dceeea95d85718
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 192.168.1.8:500, Remote: 192.168.1.3:500
  Lifetime: Expires in 3830 seconds
  Peer ike-id: 192.168.1.3
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : md5
   Encryption            : 3des-cbc
   Pseudo random function: hmac-md5
  Traffic statistics:
   Input  bytes  :               107948
   Output bytes  :               109730
   Input  packets:                 1249
   Output packets:                 1278
  Flags: Caller notification sent
  IPSec security associations: 10 created, 2 deleted
  Phase 2 negotiations in progress: 0
```

   c. If tunnel failed to be established the best practice would be to configure traceoptions with the flag ALL and monitor kmd log file for error messages, some of which we have mentioned in Task 1 of this chapter.

```
[edit security ike traceoptions]
lab@srx8# set flag ?
Possible completions:
  all                  Trace everything
  certificates         Trace certificate events
  config               Trace configuration download processing
  database             Trace security associations database events
  general              Trace general events
  high-availability    Trace high-availability operations
```

```
  ike                   Trace IKE module processing
  next-hop-tunnels      Trace next-hop-tunnels operations
  parse                 Trace configuration processing
  policy-manager        Trace policy manager processing
  routing-socket        Trace routing socket messages
  thread                Trace thread processing
  timer                 Trace internal timer events
```

2) The `show security ipsec` command also provides you with the variety of possible completions.

   a. The "security-associations" completion can give you either a brief overview or detailed report about individual IP SA. This command is a good way to verify if Phase2 is successfully completed.

```
lab@srx8> show security ipsec security-associations
Total active tunnels: 1
ID  Gateway       Port   Algorithm     SPI       Life:sec/kb  Mon    vsys
<2  192.168.1.3   500    ESP:3des/md5  39008dda  1257/  4000  -      root
>2  192.168.1.3   500    ESP:3des/md5  a9c45cf1  1257/  4000  -      root

lab@srx8> show security ipsec security-associations detail
  Virtual-system: root
  Local Gateway: 192.168.1.8, Remote Gateway: 192.168.1.3
  Local Identity: ipv4_subnet(any:0,[0..7]=192.168.10.0/24)
  Remote Identity: ipv4_subnet(any:0,[0..7]=172.16.100.0/24)
    DF-bit: clear
    Policy-name: ipsec-out

    Direction: inbound, SPI: 39008dda, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 927 seconds
    Lifesize Remaining:  4000 kilobytes
    Soft lifetime: Expires in 302 seconds
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-md5-96, Encryption: 3des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64

    Direction: outbound, SPI: a9c45cf1, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 927 seconds
    Lifesize Remaining:  4000 kilobytes
    Soft lifetime: Expires in 302 seconds
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-md5-96, Encryption: 3des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64
```

   b. The command below can give you the general idea of security protocols functionality either for individual security associations or as a summary of all of them.

```
[edit]
lab@srx8# run show security ipsec statistics
ESP Statistics:
  Encrypted bytes:          2118544
  Decrypted bytes:          1279280
  Encrypted packets:          15909
  Decrypted packets:          15730
AH Statistics:
```

```
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

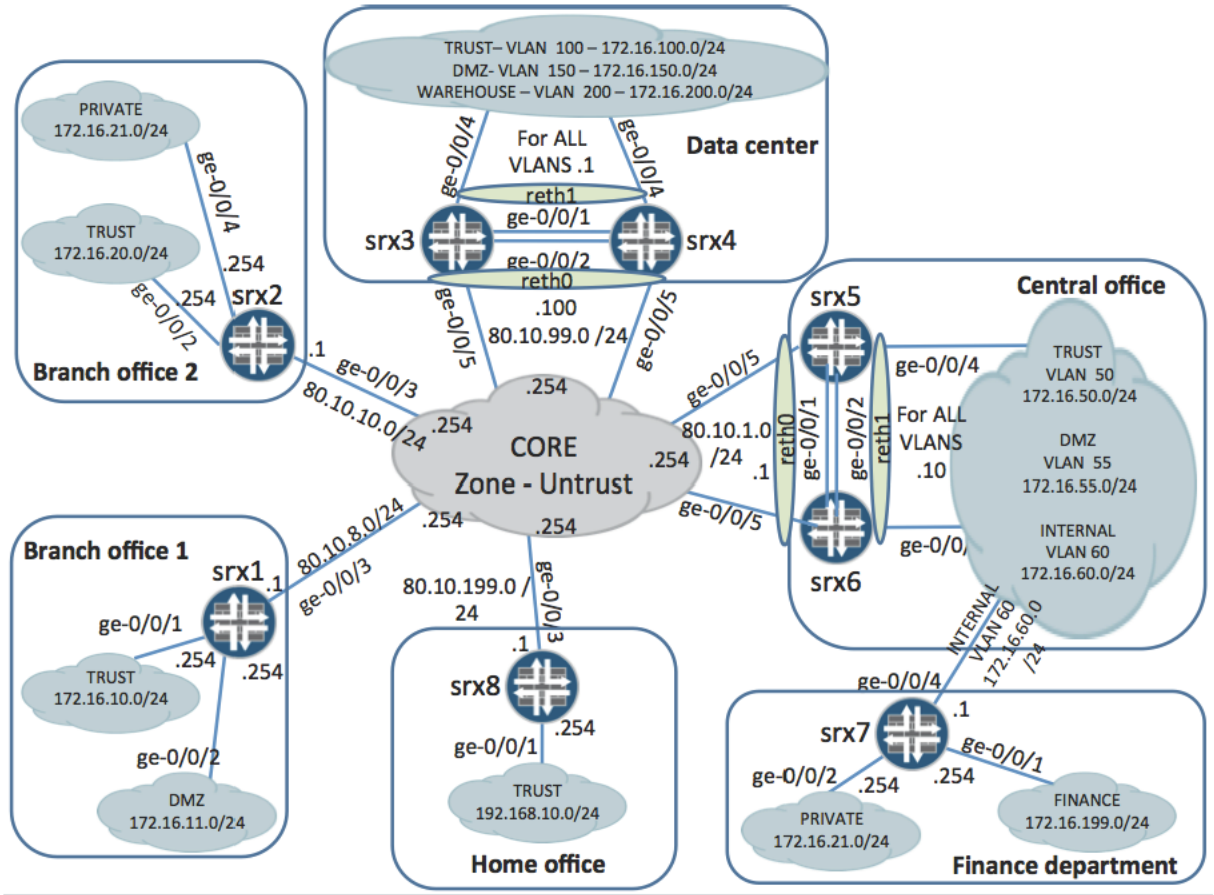
c. If you observe successful Phase1 establishment but IPSec tunnel is not available yet it is a time to start using traceoptions and monitor kmd log for any possible issues. We have mentioned some this issues previously in this chapter's task 1.

```
[edit security ipsec traceoptions]
lab@srx8# set flag ?
Possible completions:
  all                  Trace with all flags enabled
  next-hop-tunnel-binding  Trace next-hop tunnel binding events
  packet-drops         Trace packet drops
  packet-processing    Trace data packet processing events
  security-associations  Trace security association management events
```

Appendix - Chapter six: NAT

This appendix provides the solution details for the Network address translation (NAT) chapter. The configuration contains source NAT, destination NAT and static NAT.

Topology for chapter six:



Task 1: Source NAT

This section contains the details about the source NAT configuration on devices srx1, srx2 and srx8.

The solutions listed in this chapter rely on the existing security policy configuration present on the devices. If any additional security policy configuration is needed it will be shown in the respective step.

Home office: srx8

1) As instructed by task the connections from hosts in the 192.168.10.0/24 subnet (TRUST zone) have to be translated when connecting to the prefixes in the Core network (80.10.0.0/16). As it is not given which IP address to use the easiest and simplest option would be the IP address of the outgoing interface. Another alternative could be source NAT translation using an address pool.
   Here the source NAT rule-set condition will be "from zone TRUST to zone UNTRUST" and the subnet ranges above will be used in the rule match condition.
2) This indicates persistent NAT (formerly cone NAT) is meant. The persistent NAT requires the port translation to be disabled even if the egress interface's IP address is being used for translation. The type of persistent NAT here is the "target-host" option as the external hosts can contact the internal ones only after they have received any packet from them. In addition this task tells to set the inactivity-timeout to 1 hour (3600 seconds).

NOTE: During the time when the persistent sessions are maintained the connections initiated in the reverse direction (e.g. from the external hosts to the internal host's reflexive address) are allowed. No explicit security policy configuration is needed as the security policy search is bypassed and the sessions will match the same security policy as the connections from the internal zone to the external one.

```
[edit security nat source]
lab@srx8# show
interface {
    port-overloading off;
}
rule-set src-persistent-NAT {
    from zone TRUST;
    to zone UNTRUST;
    rule persistent-to-trust {
        match {
            source-address 192.168.10.0/24;
            destination-address 80.10.0.0/16;
        }
        then {
            source-nat {
                interface {
                    persistent-nat {
                        permit target-host;
                        inactivity-timeout 3600;
                    }
                }
            }
```

```
        }
    }
}
```

Branch office 1: srx1

3) The connections from the TRUST zone (subnet 172.16.10.0/24) to the Core networks (zone UNTRUST and subnet 80.10.0.0/16) have to be translated.
   The connections from the DMZ zone (subnet 172.16.11.0/24) to the Data center and Central office networks (zone UNTRUST and subnets 80.10.99.0/24 and 80.10.1.0/24) have to be translated as well.
   The source NAT rule-sets conditions will be "from zone TRUST to zone UNTRUST" and "from zone DMZ to zone UNTRUST".
   Additional translation specifics are listed in the next steps.
4) For sessions from the TRUST zone (subnet 172.16.10.0/24):
   a. Address pool 80.10.8.16/28 has to be used for translation and the PAT (port translation) has to be disabled (the "port no-translation" configuration within the address pool does that).
   b. Junos allows defining so called "overflow-pool" (also egress interface IP address can be used) to aid in situation when the used pool is exhausted. The instructions in this step define to use the egress interface IP address.

NOTE: The linked pools or egress interface must have port translation enabled.

```
[edit security nat source]
lab@srx1# show
pool src-NAT-trust {
    address {
        80.10.8.16/28;
    }
    port no-translation;
    overflow-pool interface;
}
…
rule-set src-NAT-trust-untrust {
    from zone TRUST;
    to zone UNTRUST;
    rule trust-to-untrust {
        match {
            source-address 172.16.10.0/24;
            destination-address 80.10.0.0/16;
        }
        then {
            source-nat {
                pool {
                    src-NAT-trust;
                }
            }
        }
    }
}
```

c. The 172.16.11.201 172.16.11.206 address pool has to be used for connections from the TRUST zone to the DMZ zone. Port translation is allowed here. Another rule-set needs to be created for this purpose with the condition “from zone TRUST to zone DMZ”.

```
[edit security nat source]
lab@srx1# show pool trust-to-dmz
address {
    172.16.11.201/32 to 172.16.11.206/32;
}

[edit security nat source]
lab@srx1# show rule-set src-NAT-trust-to-dmz
from zone TRUST;
to zone DMZ;
rule trust-to-dmz {
    match {
        source-address 172.16.10.0/24;
    }
    then {
        source-nat {
            pool {
                trust-to-dmz;
            }
        }
    }
}
```

5) For sessions from the DMZ zone (subnet 172.16.11.0/24):

a. 80.10.8.64/27 address pool with allowed port translation is used for connections destined to the Data center and Central office public addresses.

```
[edit security nat source]
lab@srx1# show pool src-NAT-dmz
address {
    80.10.8.64/27;
}


[edit security nat source]
lab@srx1# show rule-set src-NAT-dmz-untrust
from zone DMZ;
to zone UNTRUST;
rule dmz-to-dc-and-co {
    match {
        source-address 172.16.11.0/24;
        destination-address [ 80.10.99.0/24 80.10.1.0/24 ];
    }
    then {
        source-nat {
            pool {
                src-NAT-dmz;
            }
        }
```

```
    }
}
```

b. Sessions from DMZ zone to TRUST zone are translated using the 172.16.10.97 172.16.10.110 address range with disabled PAT. To perform this translation another rule-set needs to be configured (the condition will be "from zone DMZ to zone TRUST")

c. If pool of IP addresses is exhausted the egress interface's IP address must be used for translation;

```
[edit security nat source]
lab@srx1# show pool dmz-to-trust
address {
    172.16.10.97/32 to 172.16.10.110/32;
}
port no-translation;
overflow-pool interface;

[edit security nat source]
lab@srx1# show rule-set srx-NAT-dmz-to-trust
from zone DMZ;
to zone TRUST;
rule dmz-to-trust {
    match {
        source-address 172.16.11.0/24;
    }
    then {
        source-nat {
            pool {
                dmz-to-trust;
            }
        }
    }
}
```

The current security policy configuration does not allow traffic to pass from DMZ zone to TRUST zone. Therefore new security policy needs to be defined. Below is an configuration example using the existing address entries and defining any application.

```
[edit security policies from-zone DMZ to-zone TRUST]
lab@srx1# show
policy dmz-to-trust {
    match {
        source-address dmz-range;
        destination-address trust-address-range;
        application any;
    }
    then {
        permit;
    }
}
```

d. To ensure that connections initiated from the same host will be translated to the same IP address the "address-persistent" parameter has to be defined.

NOTE: The "address-persistent" parameter is configured globally for the whole source NAT configuration and therefore affects all source NAT translations.

```
[edit security nat source]
lab@srx1# set address-persistent
```

NOTE: In some cases such as the next device does not automatically build the ARP entries the proxy-arp needs to be configured with the IP addresses of the source pools.

Branch office 2: srx2

6) Below is the appropriate address pool configuration.

```
[edit security nat source]
lab@srx2# show
pool src-NAT-pool {
    address {
        80.10.10.128/25;
    }
}
```

One way to accomplish this task is to define two source NAT rule-sets defined with following conditions:

Rule-set "src-NAT-trust-to-untrust" --> from zone TRUST to zone UNTRUST
Rule-set "src-NAT-private-to-untrust" --> from zone PRIVATE to zone UNTRUST

Because the match criteria can contain only subnet definitions (IP addresses and masks) multiple subnet definitions are required to cover the given ranges 172.16.20.200 - 172.16.20.209 and 172.16.21.16 172.16.21.71.

172.16.20.200 - 172.16.20.209

- 172.16.20.200 - 172.16.20.207 --> 172.16.20.200/29
- 172.16.20.208 --> 172.16.20.208/32
- 172.16.20.209 --> 172.16.20.209/32

172.16.21.16 172.16.21.71

- 172.16.21.16 172.16.21.31 --> 172.16.21.16/28
- 172.16.21.32 172.16.21.63 --> 172.16.21.32/27
- 172.16.21.64 172.16.21.71 --> 172.16.21.64/29

```
[edit security nat source]
lab@srx2# show
pool src-NAT-pool {
    address {
        80.10.10.128/25;
    }
}
rule-set src-NAT-trust-to-untrust {
    from zone TRUST;
    to zone UNTRUST;
```

```
    rule IPs-200-207 {
        match {
            source-address [ 172.16.20.200/29 172.16.20.208/32
172.16.20.209/32 ];
            destination-address 80.10.0.0/16;
        }
        then {
            source-nat {
                pool {
                    src-NAT-pool;
                }
            }
        }
    }
}
rule-set src-NAT-private-to-untrust {
    from zone PRIVATE;
    to zone UNTRUST;
    rule IPs-16-71 {
        match {
            source-address [ 172.16.21.16/28 172.16.21.32/27
172.16.21.64/29 ];
            destination-address 80.10.0.0/16;
        }
        then {
            source-nat {
                pool {
                    src-NAT-pool;
                }
            }
        }
    }
}
```

7) Defining the "address-persistent" parameter assures all parallel connections from one internal host will be translated to the same IP address.

```
[edit security nat source]
lab@srx2# set address-persistent
```

8) As instructed all remaining connections should be translated using the IP address of the egress interface. This can be achieved by adding one rule with appropriate match condition and action to each of the existing rule-sets. The new rules need to be placed at the end within each rule-set to be evaluated as last.

```
[edit security nat source]
lab@srx2# show
address-persistent;
pool src-NAT-pool {
    address {
        80.10.10.128/25;
    }
```

```
}
rule-set src-NAT-trust-to-untrust {
    from zone TRUST;
    to zone UNTRUST;
    rule IPs-200-207 {
        match {
            source-address [ 172.16.20.200/29 172.16.20.208/32
172.16.20.209/32 ];
            destination-address 80.10.0.0/16;
        }
        then {
            source-nat {
                pool {
                    src-NAT-pool;
                }
            }
        }
    }
    rule all-other-trust {
        match {
            source-address 0.0.0.0/0;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
rule-set src-NAT-private-to-untrust {
    from zone PRIVATE;
    to zone UNTRUST;
    rule IPs-16-71 {
        match {
            source-address [ 172.16.21.16/28 172.16.21.32/27
172.16.21.64/28 ];
            destination-address 80.10.0.0/16;
        }
        then {
            source-nat {
                pool {
                    src-NAT-pool;
                }
            }
        }
    }
    rule all-other-private {
        match {
            source-address 0.0.0.0/0;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
```

}

The current security policies do allow connections from the TRUST and PRIVATE zones only to specific corporate networks. In order to allow connections also to other destinations new security policies need to be created.

For simplicity the security policies will allow any any any connections from these zones as the focus in this chapter is on NAT and not security policies. To achieve this, the current security policies can be deleted in the following contexts:

from-zone TRUST to-zone UNTRUST

from-zone PRIVATE to-zone UNTRUST

And new security policies should be created as follows:

```
[edit security policies from-zone TRUST to-zone UNTRUST]
root@srx2# show
policy allow-all {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

[edit security policies from-zone PRIVATE to-zone UNTRUST]
root@srx2# show
policy allow-everything {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```

Task 2: Destination NAT

This part contains details about the destination NAT configuration on the cluster 1 located in the Data center.

The initial security policy configuration is assumed. If any additional security policy is needed the configuration will be presented in the respective step.

Data center: cluster 1

1) 80.10.99.101 and 80.10.99.102 public addresses are used by the external devices for accessing the protected resources. As the connections come from the Core network the destination NAT rule-set condition will be "from zone UNTRUST".
   The subsequent steps provide more details about the required NAT destination behaviour. The 80.10.99.101 IP address has to be translated to the 172.16.100.1 IP address. The destination ports have to remain the same, e.g. PAT will not be performed. The destination NAT address pool will contain only one IP address (172.16.100.1) without any port reference. The destination IP address in the rule match criteria will be 80.10.99.101.

```
{primary:node0}[edit security nat destination]
lab@srx3# show
pool ip-172-16-100-1 {
    address 172.16.100.1/32;

}
```

2) In addition only hosts from the Home office and Branch office 1 and 2 have to be translated. The matching criterion here needs to reflect the correct source IP addresses of the connections from the Home and Branch offices, as their security devices perform source NAT.
   a. Connections from Home office have the following source address: 80.10.199.1 (the IP address of the egress interface is used see step 1)
   b. Connections from Branch office 1 use 80.10.8.16/28, 80.10.8.64/27 or 80.10.8.1 (egress interface is defined as overflow-pool in step 4.b.) IP addresses.
   c. Connections from Branch office 2 use 80.10.10.128/25 or 80.10.10.1 IP addresses.

```
{primary:node0}[edit security nat destination]
lab@srx3# show rule-set public-access
from zone UNTRUST;
rule ip-80-10-99-101 {
    match {
        source-address [ 80.10.199.1/32 80.10.8.16/28 80.10.8.64/27
80.10.8.1/32 80.10.10.128/25 80.10.10.1/32 ];
        destination-address 80.10.99.101/32;
    }
    then {
        destination-nat pool ip-172-16-100-1;
    }
}
```

3) The table below lists the required mappings of the 80.10.99.102 IP address:

Public IP address	Public port number	Private IP address	Private port number

80.10.99.102	21	172.16.100.1	21
80.10.99.102	23	172.16.150.1	23
80.10.99.102	8080	172.16.200.1	80

As it can be seen from the table the port translation needs to be done. The destination NAT will contain 3 address pools, each referencing 1 IP address and port combination from the table.

```
{primary:node0}[edit security nat destination]
lab@srx3# show
…
pool ip-172-16-100-1-port-21 {
    address 172.16.100.1/32 port 21;
}
pool ip-172-16-150-1-port-23 {
    address 172.16.150.1/32 port 23;
}
pool ip-172-16-200-1-port-80 {
    address 172.16.200.1/32 port 80;
}
```

The destination NAT rule-set from the previous step can be reused, just new rules will be added to it. The match criteria in the new rules will contain only destination address and port combination as no restrictions were given for the source address. The reordering here is not necessary as the criteria do not overlap.

```
{primary:node0}[edit security nat destination rule-set public-
access]
lab@srx3# show
from zone UNTRUST;
rule ip-80-10-99-101 {
    match {
        source-address [ 80.10.199.1/32 80.10.8.16/28 80.10.8.64/27
80.10.8.1/32 80.10.10.128/25 80.10.10.1/32 ];
        destination-address 80.10.99.101/32;
    }
    then {
        destination-nat pool ip-172-16-100-1;
    }
}
rule ip-80-10-99-102-port-21 {
    match {
        destination-address 80.10.99.102/32;
        destination-port 21;
    }
    then {
        destination-nat pool ip-172-16-100-1-port-21;
    }
}
rule ip-80-10-99-103-port-23 {
    match {
        destination-address 80.10.99.102/32;
        destination-port 23;
    }
    then {
```

```
            destination-nat pool ip-172-16-150-1-port-23;
        }
    }
    rule ip-80-10-99-102-port-8080 {
        match {
            destination-address 80.10.99.102/32;
            destination-port 8080;
        }
        then {
            destination-nat pool ip-172-16-200-1-port-80;
        }
    }
```

4) Junos can check within security policies whether a NAT translation was performed on the packet or not and based on the result handle the packet as desired (permit, deny, etc.). Additional security policies are needed because the existing ones on the cluster 1 do not handle traffic destined to the 80.10.99.101 and 80.10.99.102 addresses.
The criteria in the security policies can contain specific source, destination IP addresses as well as specific set of applications. However in this case it is sufficient to base the criteria only on the destination IP addresses (172.16.100.1, 172.16.150.1, 172.16.200.1) and the checking whether the packet was translated or not.

NOTE: Because the destination NAT is executed before security policies the security policies criteria need to consider the changed packets, e.g. use translated addresses.

Appropriate address book entries need to be created in respective zones. Below are shown all address-book entries for the affected zones not just the new ones.

```
{primary:node0}[edit security]
lab@srx3# show zones security-zone TRUST address-book
address trust-address-range 172.16.100.0/24;
address ip-172.16.100.1 172.16.100.1/32;

{primary:node0}[edit security]
lab@srx3# show zones security-zone DMZ address-book
address dmz-range 172.16.150.0/24;
address ip-172.16.150.1 172.16.150.1/32;

{primary:node0}[edit security]
lab@srx3# show zones security-zone WAREHOUSE address-book
address warehouse-range 172.16.200.0/24;
address ip-172.16.200.1 172.16.200.1/32;
```

The next step is to create the security policies. As these security policies have very specific criteria (host destination IP address) they should be placed on top of the security policies list in each context of zones to be evaluated first:

- from UNTUST to TRUST
- from UNTUST to DMZ
- from UNTUST to WAREHOUSE

The reordering of security policies is achieved using the “insert” command.

The permit action allows defining whether translated or untranslated packets should be dropped.

```
{primary:node0}[edit security policies from-zone UNTRUST to-zone
TRUST]
lab@srx3# show
policy public-TRUST {
    match {
        source-address any;
        destination-address ip-172.16.100.1;
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
        }
    }
}
```

```
{primary:node0}[edit security policies from-zone UNTRUST to-zone
DMZ]
lab@srx3# show
policy public-DMZ {
    match {
        source-address any;
        destination-address ip-172.16.150.1;
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
        }
    }
}
policy access-from-corp{
…
```

```
{primary:node0}[edit security policies from-zone UNTRUST to-zone
WAREHOUSE]
lab@srx3# show
policy public-WAREHOUSE {
    match {
        source-address any;
        destination-address ip-172.16.200.1;
        application any;
    }
    then {
```

```
        permit {
            destination-address {
                drop-untranslated;
            }
        }
    }
}
policy co-dmz-warehouse {
…
```

5) Interface based source NAT has to be defined in order for the hosts within the TRUST zone to think the traffic was sent from cluster 1 itself. The rule-set condition will be "from routing instance default to zone TRUST" co cover all traffic going to TRUST zone. The rule match criteria will list the destination address range 172.16.100.0/24 and the then statement will reference the interface.

```
{primary:node0}[edit security nat source]
lab@srx3# show
rule-set traffic-to-TRUST {
    from routing-instance default;
    to zone TRUST;
    rule traffic-to-trust-zone {
        match {
            destination-address 172.16.100.0/24;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
```

NOTE: Because the used IP addresses for destination NAT are from the same range as the IP address on the incoming interface the proxy-ARP needs to be configured.

```
{primary:node0}[edit security nat proxy-arp]
lab@srx3# show
interface reth0.0 {
    address {
        80.10.99.101/32 to 80.10.99.102/32;
    }
}
```

Task 3: Static NAT

This section presents the static NAT configuration details on the cluster 2 and srx7.

Central office: cluster 2

1) Static NAT provides bidirectional address translation, e.g. combination of source and destination NAT. Based on the given requirements this type of translation should be provided for the srx7 loopback IP address. The mapping here is 80.10.1.11/32 <--> 192.168.1.7/32 and the rule-set condition is "from zone UNTRUST". Below is the static NAT configuration from cluster 2.

```
{primary:node0}[edit security nat static]
lab@srx5# show
rule-set srx7-loopback {
    from zone UNTRUST;
    rule srx7-loopback-IP {
        match {
            destination-address 80.10.1.11/32;
        }
        then {
            static-nat prefix 192.168.1.7/32;
        }
    }
}
```

Two appropriate security policies have to be created to allow srx7 to initiate and accept connections to and from its loopback interface. First security policy will be from UNTRUST zone to INTERNAL zone with the following criteria: source address any, destination address 192.168.1.7/32 and application any. The second policy will be for the sessions in reverse direction, e.g. from INTERNAL zone to UNTRUST zone with the following criteria: source address 192.168.1.7/32, destination address any and application any. In this particular case no policy reordering is needed as the existing policies do not overlap with the new ones.

```
{primary:node0}[edit security zones security-zone INTERNAL]
lab@srx5# set address-book address srx7-loopback 192.168.1.7/32

{primary:node0}[edit security policies from-zone UNTRUST to-zone
INTERNAL]
lab@srx5# show
policy srx-loopback-access {
    match {
        source-address any;
        destination-address srx7-loopback;
        application any;
    }
    then {
        permit;
    }
}


{primary:node0}[edit security policies from-zone INTERNAL to-zone
UNTRUST]
```

```
lab@srx5# show policy srx7-loopack-initiated
match {
    source-address srx7-loopback;
    destination-address any;
    application any;
}
then {
    permit;
}
```

2) Similarly as in the previous step static NAT will be use for mapping the following ranges 80.10.1.128/29 <--> 172.16.55.128/29. Here the rule-set condition can be "from routing-instance default" to allow hosts from any network to connect to the protected resources using the 80.10.1.128/29 IP addresses. The exiting security policies define in more details who will have access to which protected resources.

```
{primary:node0}[edit security nat static]
lab@srx5# show rule-set dmz-access
from routing-instance default;
rule dmz-access-172-16-55-128 {
    match {
        destination-address 80.10.1.128/29;
    }
    then {
        static-nat prefix 172.16.55.128/29;
    }
}
```

NOTE: The proxy-arp needs to be configured for the static NAT as well.

```
{primary:node0}[edit security nat proxy-arp]
lab@srx5# show
interface reth0.0 {
    address {
        80.10.1.128/29;
        80.10.1.11/32;
    }
}
```

NOTE: A static route needs to be defined to provide connectivity to the srx7's lo0 IP address:

```
{primary:node0}[edit]
root@srx5# set routing-options static route 192.168.1.7/32 next-hop
172.16.60.1
```

Finance department: srx7

3) Hiding the given address can be done using again static NAT translation. The static NAT allows defining one-to-one mappings between subnets (or networks). This mapping is based on address shifting, e.g. 1^{s} IP address of public range is mapped to the 1^{s} IP address of the

private range,2 d IP address of public range is mapped to the 2 d IP address of the private range, etc.

The address range for translation needs to be split because the address ranges to be hidden are smaller. The instructions tell the mappings have to start with these IP addresses: 172.16.60.128 <--> 172.16.21.0. Based on this information the subnets will be mapped as follows:

172.16.60.128/26 <--> 172.16.21.0/26

172.16.60.192/26 <--> 172.16.199.0/26

One static NAT rule-set will be sufficient to provide both mapping and will have the condition "from zone INTERNAL".

```
[edit security nat static]
lab@srx7# show
rule-set PRIVATE-FINANCE-static-NAT {
    from zone INTERNAL;
    rule PRIVATE-static-NAT {
        match {
            destination-address 172.16.60.128/26;
        }
        then {
            static-nat prefix 172.16.21.0/26;
        }
    }
    rule FINANCE-static-NAT {
        match {
            destination-address 172.16.60.192/26;
        }
        then {
            static-nat prefix 172.16.199.0/26;
        }
    }
}
```

In this case the proxy-arp configuration is needed too.

```
[edit security nat proxy-arp]
lab@srx7# show
interface ge-0/0/4.60 {
    address {
        172.16.60.128/25;
    }
}
```

4) Due the processing sequence, checking if the packets were or weren't translated can be done only for sessions where destination NAT was performed. (Destination NAT is done before and source NAT is done after security policies.). Because the existing policies on the srx7 device do not allow any traffic going from the INTERNAL zone to the FINANCE (or PRIVATE) zone new security policies that will allow only translated traffic to pass need to be created. Below are the security policies details.
   a. First policy:
      i. From zone INTERNAL to zone FINANCE

- Criteria: source address any, destination address 172.16.199.0/26, application any

The existing policies will be used to determine whether to allow or deny the connections in opposite the direction.

```
[edit security zones security-zone FINANCE]
lab@srx7# set address-book address FINANCE-static-NAT
172.16.199.0/26

[edit security policies from-zone INTERNAL to-zone FINANCE]
lab@srx7# show
policy FINANCE-access {
    match {
        source-address any;
        destination-address FINANCE-static-NAT;
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
        }
    }
}
```

b. Second policy:

ii. From zone INTERNAL to zone PRIVATE

- Criteria: source address any, destination address 172.16.21.0/26, application any

iii. A security policy that allows connections in the reverse direction from PRIVATE to INTERNAL zone.

- Criteria: source address 172.16.21.0/26, destination address any, application any

```
[edit security zones security-zone PRIVATE]
lab@srx7# set address-book address PRIVATE-static-NAT 172.16.21.0/26

[edit security policies from-zone INTERNAL to-zone PRIVATE]
lab@srx7# show
policy PRIVATE-access {
    match {
        source-address any;
        destination-address PRIVATE-static-NAT;
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
        }
```

```
    }
}

[edit security policies from-zone PRIVATE to-zone INTERNAL]
root@srx7# show
policy access-from-PRIVATE-static-NAT {
    match {
        source-address PRIVATE-static-NAT;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```

NOTE: The configuration on the cluster2 allows connections to the srx7 loopack IP address, but the current srx7 configuration does not. The following tasks need to be done to provide that:

- Assign lo0 to a security zone
- Create appropriate security policies

For simplicity sake the lo0 interface will be assigned to the INTERNAL zone and a new security policy that allows intrazone traffic within the INTERNAL zone will be created.

```
[edit security zones security-zone INTERNAL]
root@srx7# set interfaces lo0.0 host-inbound-traffic system-
services all

[edit security zones security-zone INTERNAL]
root@srx7# set interfaces lo0.0 host-inbound-traffic protocols
all

[edit security policies from-zone INTERNAL to-zone INTERNAL]
root@srx7# show
policy intrazone-INTERNAL-traffic {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```

Task 4: NAT Protocol Translation (IPv6/IPv4)

This section focuses on enabling IPv6 and IPv4 hosts to communicate with each other by using NAT.

Branch 2

1) Configure the following IPv6 network for the PRIVATE zone: 2001:a11::254/64. Ensure the Branch2 device can reach IPv6 host 2001:a11::1/128 on interface ge-0/0/4.

```
root@srx2# show interfaces ge-0/0/4
unit 0 {
    ...
    family inet6 {
        address 2001:a11::254/64;
    }
}

root@srx2# show security forwarding-options
family {
    inet6 {
        mode flow-based;
    }
}
```

Ensure that your reboot the Branch2 device

2) Ensure that IPv6 host 2001:a11::1/128 attached to the PRIVATE zone in Branch2 can reach the IPv4 host 80.10.10.100 by sending and receiving traffic to and from IPv6 address: 2001:a11::253. Modify or change your (existing) policies to allow traffic between the hosts

3) Ensure that IPv4 host 80.10.10.254 attached in the UNTRUST zone can reach IPv6 host 2001:a11::1 by sending and receiving traffic to and from IPv4 address 80.10.10.2 Modify or change your (existing) policies to allow traffic between the hosts

```
security {
    nat {
        source {
            pool v4v6 {
                address {
                    2001:a11::253/128;
                }
            }
            pool v6v4 {
                address {
                    80.10.10.2/32;
```

```
            }
        }
        rule-set src-NAT-private-to-untrust {
            from zone PRIVATE;
            to zone UNTRUST;
            rule 64nat {
                match {
                    source-address 2001:a11::1/128;
                    destination-address 80.10.10.100/32;
                }
                then {
                    source-nat {
                        pool {
                            v6v4;
                        }
                    }
                }
            }
        rule-set src-NAT-untrust-to-private {
            from zone UNTRUST;
            to zone PRIVATE;
            rule 46nat {
                match {
                    source-address 80.10.10.254/32;
                    destination-address 2001:a11::1/128;
                }
                then {
                    source-nat {
                        pool {
                            v4v6;
                        }
                    }
                }
            }
        }
    }
    static {
        rule-set v4-2-v6 {
            from zone UNTRUST;
            rule natpt-1 {
                match {
                    destination-address 80.10.10.2/32;
                }
                then {
                    static-nat {
                        prefix {
                            2001:a11::1/128;
                        }
```

```
                        }
                    }
                }
            }
            rule-set v6-2-v4 {
                from zone PRIVATE;
                rule natpt-2 {
                    match {
                        destination-address 2001:a11::253/128;
                    }
                    then {
                        static-nat {
                            prefix {
                                80.10.10.100/32;
                            }
                        }
                    }
                }
            }
        }
        proxy-arp {
            interface ge-0/0/3.0 {
                address {
                    80.10.10.2/32;
                }
            }
        }
        proxy-ndp {
            interface ge-0/0/4.0 {
                address {
                    2001:a11::253/128;
                }
            }
        }
    }
```

Allow the traffic

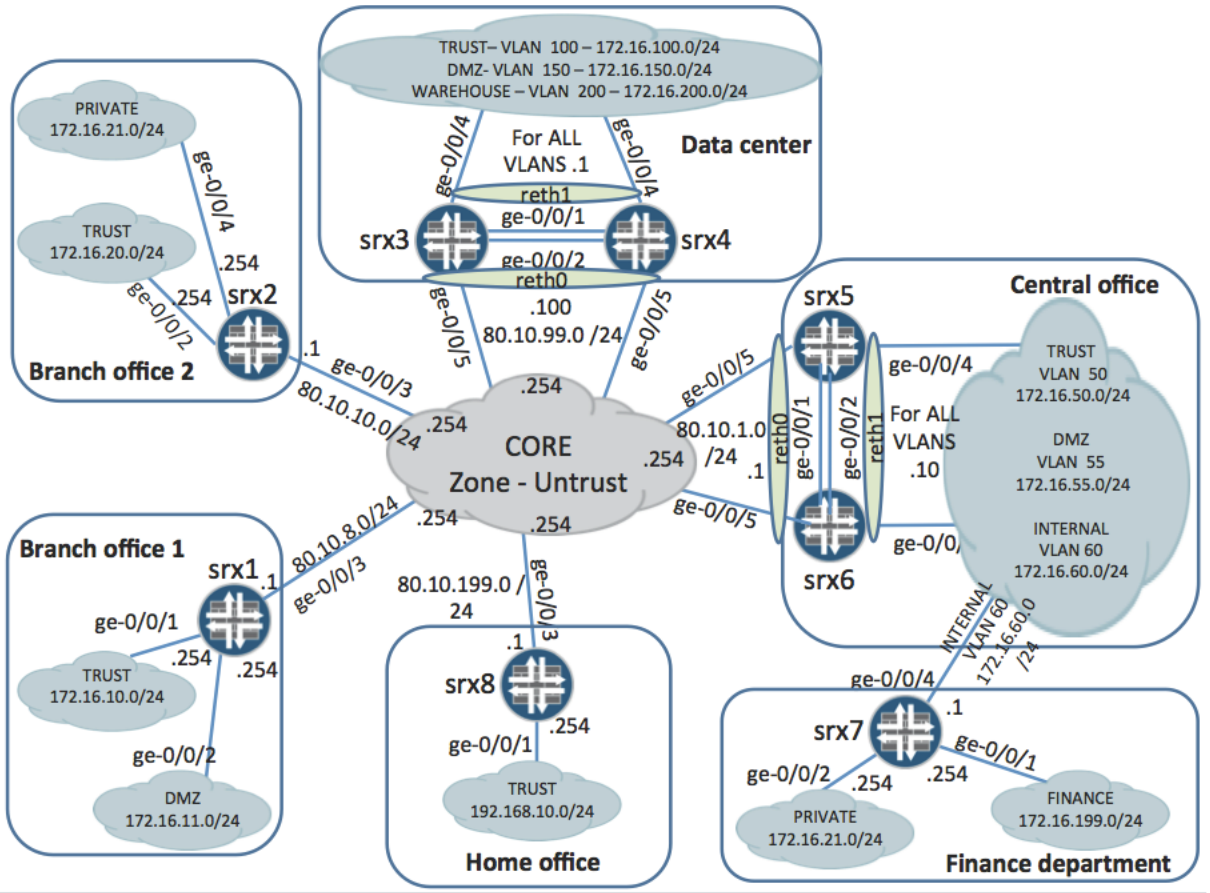
```
root@srx2# show security policies
from-zone PRIVATE to-zone UNTRUST {
    policy allow-everything {
        match {
            source-address any;
            destination-address any;
            application any;
        }
```

```
            then {
                permit;
            }
        }
    }
    from-zone UNTRUST to-zone PRIVATE {
        policy allow-everything {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
```

Chapter seven: Attack Prevention and Mitigation

This chapter is dedicated to the Attack Prevention and Mitigation functionality on Junos security devices. The presented tasks will require you to configure stateless packet filtering, SCREEN functionality and Intrusion Prevention System features set.

Topology for chapter seven:



Task 1: Firewall Filters

In this part you will configure stateless packet filters on all security devices in the lab. The goal of this task is to protect every security device's control plane from malicious traffic by applying Firewall Filters to devices loopback interfaces.

Firewall filter works similarly to security policies in way of matching traffic patterns and applying actions. The main difference is it works in the stateless manner and needs to be applied to ingress or egress interfaces.

In case of this task firewall filter is managing traffic destined to the control plane and need to be applied as an input filter to the loopback interface.

You could find that task is quite complicated until you follow simple approach.Highlight main traffic types and group themin such a way that the key elements can be described by simple conditional clauses. That will allow you creating building blocks of your desired firewall filter.

As soon as all bricks are ready you just need to place them in correct order. Term's order does a crucial matter because matching criteria look up is going from the top to the bottom till first match! You must avoid having terms with general matching criteria on the top of you firewall filter.

1) Ensure that IPSec tunnels can be established for all security devices in the network regardless if they are located in front of or behind NAT devices. All security devices are using ESP as an IPSec protocol.

In our labs we use only ESP as an IPSec protocol so it must be matched in the "`from`" statement. The UDP port 500 needs to be opened for the IKE communications in normal circumstance and UDP port 4500 in case if VPN gateway is located behind NAT device.

```
[edit firewall family inet filter protect-lo0 term ipsec]
lab@srx8# show
from {
    source-address {
        80.10.0.0/16;
    }
    protocol [ esp udp ];
    port [ 500 4500 ];
}
then accept;
```

2) Ensure that OSPF protocol is permitted for of the range of IP addresses allocated for tunnel interfaces;

The configuration excerpt below allows OSPF traffic coming from st0 interfaces configured in other security devices.

```
[edit firewall family inet filter protect-lo0 term ospf]
lab@srx8# show
from {
    source-address {
        11.0.0.0/24;
    }
```

```
    protocol ospf;
}
then accept;
```

3) Permit DNS on UDP port 53 and NTP traffic originated from the IP address 172.31.10.1;
4) Permit SNMP, Radius, http/https, telnet and ftp traffic originated from the out-of-band management network 10/8;

The configuration of this task is looking straightforward until you start to do step 6. The ftp and http traffic are mentioned in both steps. You can create single term that would describe snmp, radius, http, https and ftp. But, in such a case, this term will shade the term that you will create later, during step 6.

The work around for this issue is to describe http and ftp traffic in separate term. See configuration excerpt for step 6.

5) Permit ping packets regardless of the source IP address;
6) Ensure that ftp and http traffic is rate limited to 1 Mbps with the allowed traffic burst of 100 KB;

The configuration element that allows you to rate limit particular types of traffic is a policer. Its configuration is available under the `[edit firewall]` level of hierarchy. As soon as you described the way in which traffic must be limited you need to apply policer to the particular term as an action.

```
[edit firewall family inet filter protect-lo0 term rate-limit-ftp-
http]
lab@srx8# show
from {
    source-address {
        10.0.0.0/8;
    }
    protocol tcp;
    port [ ftp ftp-data http ];
}
then policer rate-limit-ftp-http;
```

When you deal with the policer configuration keep in mind that "`bandwidth-limit`" is measured in bits per second and "`burst-size-limit`" is measured in bytes!

```
[edit firewall policer rate-limit-ftp-http]
lab@srx8# show
if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 100k;
}
then discard;
```

7) Silently drop and syslog all other traffic.

The configuration example below combines "syslog" and "discard" actions together. In case if you do not need to syslog dropped traffic you can simply use implicit deny which is available by default for every firewall filter.

```
[edit firewall family inet filter protect-lo0 term deny-any-other]
lab@srx8# show
then {
    syslog;
    discard;
}
```

As soon as you completed the firewall filter's configuration it is a time applying it to the lo0 interface.

```
[edit interfaces lo0 unit 0]
lab@srx8# show
family inet {
    filter {
        input protect-lo0;
    }
    address 192.168.1.1/32;
}
```

Task 2: SCREEN

In this part you will configure lab equipment as necessary to protect network recourses of Branch offices, Finance department and Home office from different types of reconnaissance and DoS attacks with the SCREEN feature.

Branch office 1, Branch office 2, Home office: srx1, srx2 and srx8

Configure functionality on srx1, srx2 and srx8 to protect sites from malicious traffic arriving from the Core network:

1) Ensure that the SYN Proxy mechanism is enabled;

Your firewall can operate either in the syn-proxy or in the syn-cookie mode. Here is the example of syn-proxy configuration, which is enabled by default.

```
[edit security flow]
lab@srx8# show
syn-flood-protection-mode syn-proxy;
```

2) Protect against session table flood with the thresholds of 250 sessions per source and per destination IP addresses;

The SCREEN configuration is straightforward and can be done and verified on one security device. The "`load merge`" command will help you to complete configuration for the rest of the network sites.

The configuration excerpt below shows the how to configure session's limit.

```
[edit security screen ids-option from-core]
lab@srx8# show
limit-session {
    source-ip-based 250;
    destination-ip-based 250;
}
```

3) Configure protection against TCP SYN segments flood with the following thresholds and timer values:
    a. The destination thresholds values of 5000 TCP SYN segments per second;
    b. Ensure that security device starts SYN Proxy protection mechanism when TCP SYN segments arrival rate reaches 500 segments per second;
    c. Ensure that security device generates an alarm when TCP SYN segments arrival rate reaches 7500 segments per second;
    d. The maximum time before incomplete sessions are dropped should be 10 seconds.

The configuration excerpt below shows the how to enable protection against SYN flooding.

```
[edit security screen ids-option from-core tcp]
lab@srx8# show
syn-flood {
    alarm-threshold 7500;
    attack-threshold 500;
```

```
    destination-threshold 5000;
    timeout 10;
}
```

4) Protect against ICMP flood with the threshold of 500 packets per second;
5) Ensure that security device drops packets with following abnormalities:
    a. Fragmented ICMP packets;
    b. Fragmented TCP SYN segments.
    c. ICMP packet with size larger than 1024 bytes;

As soon as all requested protection mechanisms are enabled in the ids profile you need to apply it to the security zone from which you are expecting malicious traffic arrival.

```
lab@srx8#set security zones security-zone UNTRUST screen from-core
```

Finance department: srx7

Configure srx7 to protect site from reconnaissance attempts arriving from the INTERNAL zone:

6) Ensure that detection of malicious traffic results in alarm generation instead of dropping the packets belonging to malicious packet flow;

The configuration approach for srx7 is very similar to previously discussed settings. The main difference is the alarm flag that you need to set up in the ids option for srx7 INTERNAL zone.

```
[edit security screen ids-option protect-from-internal]
lab@srx7# show
alarm-without-drop;
```

7) Protect against IP addresses sweeps with a detection rate of 10 ICMP packets arrived per 500 ms time interval;
8) Protect against port scans with a detection rate of 10 port scans per 750 ms time interval;
9) Detect IP packets with following values in the Options field:
    a. Time stamp option
    b. Record route option
10) Protect against following operating systems probes:
    a. The TCP segment has both SYN and FIN flags set;
    b. The TCP segment has no flags set.

Task 3: Intrusion Prevention System

In this part you will configure lab equipment as necessary to deploy Intrusion Prevention System features in the Data Center and Central office.

NOTE: The initial IDP setup procedure is described in Juniper Networks KB16489 "SRX Getting Started - Quick Setup Guide for Configuring IDP on a SRX or J-Series device":

http://kb.juniper.net/InfoCenter/index?page=content&id=KB16489

Data Center: cluster1

There are several servers located in different zones in the Data Center network (see the table below). Services that are not mentioned in this table or in the following configuration tasks must be restricted by the security policies.

Security zone name	Services
TRUST	SMTP, POP3, IMAP
DMZ	HTTP, SMTP, POP3, IMAP, FTP
WAREHOUSE	HTTP

1) Configure cluster1 to use the TCP SYN cookie rather TCP SYN proxy mechanism.

Your firewall can operate either in the syn-proxy or in the syn-cookie mode. Here is the example of syn-cookie configuration.

```
[edit security flow]
lab@cluster1# show
syn-flood-protection-mode syn-cookie;
```

2) Protect the Data Center resources with the predefined IDP policy "Recommended". Ensure that only specified services are monitored for traffic traversing between the Data Center protected resources and Untrust zone.

You can configure only one active idp policy per the branch SRX and this policy must describe all traffic types that you intend to monitor regardless of security zone context. The idp policy can be modified in such a way that matching criteria would describe very specific traffic types.

The configuration excerpt below is activating Recommended idp policy.

The are few predefined policies that were installed during the initial idp setup. You need to activate Recommended idp policy. Use command "`show configuration security idp idp-policy Recommended`" to see all types of traffic that is analyzed by this policy. The policy consists of 9 predefined rules and some of them are excessive for the conditions of this task. You need to leave rules that monitor HTTP, SMTP, POP3, IMAP and FTP traffic.

```
[edit security idp]
lab@srx3# show active-policy
active-policy Recommended;
```

3) Ensure that all the Data Center resources are protected against TCP/IP attacks and malware activities from the Untrust zone as well as internal servers can't cause infection or be the source of attacks to any hosts located in the Untrust zone.

The rulebase-ips contains two more rules that are necessary for this step's conditions. These rules are:

- Rule 1 `/* This rule is designed to protect your networks against important TCP/IP attacks. */`
- Rule 9 `/* This rule is designed to protect your network against common internet malware. */`

4) Allow anonymous access from Untrust zone to the ftp servers 172.16.150.1 and 172.16.150.2 only from the 80.10.1.128/29 range. Restrict access for the rest of the hosts located in the Untrust zone. Silently drop packets from unauthorized hosts, block them for 1 hour and generate log messages with severity level Major and alert flag.

The first step assumes creation of custom attack object that describes anonymous access to ftp server.

```
[edit security idp custom-attack deny-ftp-anonymous]
lab@cluster1# show
recommended-action drop;
severity major;
attack-type {
    signature {
        context ftp-username;
        pattern "^anonymous$";
        direction client-to-server;
    }
}
```

The representation of pattern's value as the string "`^anonymous$`" means that we're looking for exact matching of the ftp user name starting (^) with "a" and ended ($) with "s".

As soon as attack object is created you can use it in the IDP policy. In example below we created one more rule in the rulebase-ips. This rule describes traffic that must be dropped.

Note that action can be specified either explicitly in the "`then`" statement of the rule or can be borrowed from the "`recommended-action`" of attack object.

```
[edit security idp idp-policy Recommended rulebase-ips rule deny-anonymous-
ftp]
lab@cluster1# show
match {
    from-zone UNTRUST;
    source-address any;
    to-zone DMZ;
    destination-address [ 172.16.150.1 172.16.150.2 ];
    application junos-ftp;
    attacks {
        custom-attacks deny-ftp-anonymous;
    }
}
then {
```

```
    action {
        recommended;
    }
    ip-action {
        ip-block;
        target source-address;
        timeout 3600;
    }
    notification {
        log-attacks {
            alert;
        }
    }
}
```

The conditions of this step define that only particular traffic sourced from the IP subnet 80.10.1.128/29 and destined to IP addresses 172.16.150.1 and 172.16.150.2 is permitted. This goal can be achieved by applying action "none" to this packet's flow.

```
[edit security idp idp-policy Recommended rulebase-exemptrule allow-
anonymous-ftp]
lab@cluster1# show
match {
    from-zone UNTRUST;
    source-address 80.10.1.128/29 ;
    to-zone DMZ;
    destination-address [ 172.16.150.1 172.16.150.2 ];
    application junos-ftp;
    attacks {
        custom-attacks deny-ftp-anonymous;
    }
}
then {
    action {
none;
    }
}
```

NOTE: Do not configure policy for acceptable traffic within rulebase-exempt. Do not apply action "ignore" instead of "none". Both of these actions will lead to the exclusion of acceptable trafficfrom the subsequent analysis that can be done by other IDP rules.

If configuration of your IDP policy is completed it is time to apply it as an action to the security policy. You do not need to specify IDP policy's name at this configuration step because only active idp policy is used.

```
[edit security policies from-zone UNTRUST to-zone DMZ]
lab@cluster1# show
policy idp-inspection {
    match {
        source-address any;
        destination-address any;
        application [ junos-http junos-smtp junos-pop3 junos-imap junos-ftp
];
    }
    then {
        permit {
            application-services {
```

```
                idp;
            }
        }
    }
}
```

Central office: cluster2

There are two servers located in the DMZ security zone in the Central office network (see table below). Services that are not mentioned in this table or in following configuration tasks must be restricted by security policies.

Server's IP address	Services
172.16.55.100	HTTP
172.16.55.200	FTP

5) Configure cluster2 to use the TCP SYN cookie rather than the TCP SYN proxy mechanism.
6) Protect the Web and the FTP servers from any kind of HTTP or FTP attacks respectively with the severity level Critical or Majorfrom everywhere. Silently drop session in the case of attack's detection, generate syslog message with the alert flag and block attacker's future connection attempts for two hours.

At this step you need to use predefined attack groups for HTTP and FTP with appropriate severity levels. In example below we created one more rule in the rulebase-ips.

```
rule rule-protect-http-ftp-servers {
    match {
        from-zone any;
        source-address any;
        to-zone DMZ;
        destination-address [ 172.16.55.100/32 172.16.55.200/32 ];
        attacks {
            predefined-attack-groups [ "FTP - Critical" "FTP - Major" "HTTP
- Critical" "HTTP - Major" ];
        }
    }
    then {
        action {
            drop-connection;
        }
        ip-action {
            ip-block;
            target source-address;
            timeout 7200;
        }
        notification {
            log-attacks {
                alert;
            }
        }
    }
}
```

7) Upload of zip, rar or tgz files to the ftp server is prohibited from anywhere. Each detected attempt results in disconnecting the client from the server by receiving with TCP RST message. The client is blocked for next five minuets. The syslog message with the severity

level Major must be generated. Clients located in the TRUST and in the INTERNAL zones are permitted to access servers located both in the UNTRUST zone and in the DMZ zone.

This example's goal is to show you how to configure compound attack object and describe traffic patterns with simple regular expressions.

The main difference between the configuration excerpt below and configuration for step 21 is the "attack-type" that is specified now as a "chain" and allows combining together few sub objects.

```
[edit security idp custom-attack upload-to-ftp]
lab@cluster2# show
severity major;
attack-type {
    chain {
        expression "zip or rar or tgz";
        member zip {
            attack-type {
                signature {
                    context ftp-put-filename;
                    pattern ".*\.\[zip\]";
                    direction client-to-server;
                }
            }
        }
```

The pattern ".*\.\[zip\]"describes all files with .zip extension. The ".*" is used as a wildcard. The "\" is used to match character ".". The \[zip\]"describes case-insensitive match.

```
        member rar {
            attack-type {
                signature {
                    context ftp-put-filename;
                    pattern ".*\.\[rar\]";
                    direction client-to-server;
                }
            }
        }
        member tgz {
            attack-type {
                signature {
                    context ftp-put-filename;
                    pattern ".*\.\[tgz\]";
                    direction client-to-server;
                }
            }
        }
    }
}
```

8) Ensure that client's machines located in the TRUST security zone are protected against worms and Trojans types of attacks of all severity levels from anywhere as well as they can't cause infection or be the source of attack for any hosts located in DMZ and INTERNAL security zones.

```
rule rule-protect-clients {
    match {
        from-zone any;
        source-address any;
```

```
        to-zone TRUST;
        destination-address any;
        attacks {
  predefined-attack-groups [ "TROJAN - All" "WORM - All" ];
        }
    }
    then {
        action {
            drop-connection;
        }
        notification {
            log-attacks {
                alert;
            }
        }
    }
}
```

Ensure that security policies between TRUST zone and DMZ and INTERNAL zones use action "application service idp" as in example below:

```
from-zone TRUST to-zone INTERNAL {
    policy trust-to-int-priv-fin {
        match {
            source-address trust-address-range;
            destination-address internal-finance-private-ranges;
            application any;
        }
        then {
            permit;
     application-services {
                        idp;
                    }
            }
        }
    }
```

9) Clients are instantly denied access to the following URLs:
   c. www.playboy.com
   d. www.hustler.com

   The connection must be closed when such attempt is detected.

```
[edit security idp custom-attack prohibited-web-sites]
lab@cluster2# show
recommended-action close;
severity major;
attack-type {
    chain {
        member playboy {
            attack-type {
                signature {
                    context http-header-host;
                    pattern ".*\.\[playboy\.com\]";
                    direction client-to-server;
                }
            }
        }
        member hustler {
```

```
            attack-type {
                signature {
                    context http-header-host;
                    pattern ".*\.\[hustler\.com\]";
                    direction client-to-server;
                }
            }
        }
    }
}
```

10) The downloading of PDF files via HTTP is prohibited for users located in the TRUST zone. If such attempt has been detected the connection has to be closed.

```
[edit security idp custom-attack download-to-clients]
lab@cluster2# show
recommended-action close;
severity major;
attack-type {
    signature {
        context http-header-content-type;
        pattern ".*\[pdf\].*";
        direction server-to-client;
    }
}
```

As soon as all attack objects and groups are defined you can combine them together into the IDP policy. You will create and activate your own policy rather than will use any of predefined IDP policies, and, as a final step, enable IDP action for the necessary security policies.

Task 4: Verification

Firewall Filters

The way that you can verify firewall filter's operations is to launch different types of traffic destined to the Routing Engine and observe the fact of the success or the failure.

You can temporary enable action count for some particular terms as a work around.

```
[edit firewall family inet filter protect-lo0 term public-services]
lab@srx8# show
from {
    source-address {
        172.31.10.1/32;
    }
    protocol udp;
    port [ ntp 53 ];
}
then {
    count public-services;
    accept;
}
```

If any traffic match the "`from`" statement you will be able to see counter incremented in the output below:

```
lab@srx8> show firewall filter protect-lo0 counter public-services
Filter: protect-lo0
Counters:
 Name                    Bytes                  Packets
 public-services         0                      0
```

SCREEN

You can verify your SCREEN configuration by launching command below.

```
lab@srx8> show security screen ids-option from-core-net
Screen object status:

Name                                        Value
  ICMP flood threshold                      500
  TCP SYN flood attack threshold            500
  TCP SYN flood alarm threshold             7500
  TCP SYN flood source threshold            4000
  TCP SYN flood destination threshold       5000
  TCP SYN flood timeout                     10
  Session source limit threshold            250
  Session destination limit threshold       250
```

If you are looking for real statistic use command "`show security screen statistics`". This command allows you deriving statistics on per interface or on per security zone base.

```
lab@srx8> show security screen statistics zone UNTRUST
```

```
Screen statistics:

IDS attack type                                 Statistics
  ICMP flood                                    0
  UDP flood                                     0
  TCP winnuke                                   0
  TCP port scan                                 0
  ICMP address sweep                            0
  TCP sweep                                     0
  UDP sweep                                     0
  IP tear drop                                  0
  TCP SYN flood                                 0
  IP spoofing                                   0
  ICMP ping of death                            0
  IP source route option                        0
  TCP land attack                               0
  TCP SYN fragment                              0
  TCP no flag                                   0
  IP unknown protocol                           0
  IP bad options                                0
  IP record route option                        0
  IP timestamp option                           0
  IP security option                            0
  IP loose source route option                  0
  IP strict source route option                 0
  IP stream option                              0
  ICMP fragment                                 0
  ICMP large packet                             0
  TCP SYN FIN                                   0
  TCP FIN no ACK                                0
  Source session limit                          0
  TCP SYN-ACK-ACK proxy                         0
  IP block fragment                             0
  Destination session limit                     0
```

Intrusion Prevention System

There are few commands below that can be used for IDP troubleshooting and monitoring.

```
lab@cluster2> show security idp status

lab@cluster2> show security idp attack table

lab@cluster2> show security flow ip-action all
```

You can verify that IDP configuration is operational or not by analyzing local file "`messages`". The best way to sift through the contents of this file is to filter syslog messages with the text string "RT_IDP".

```
lab@cluster1>show log messages | match RT_IDP | match severity
```

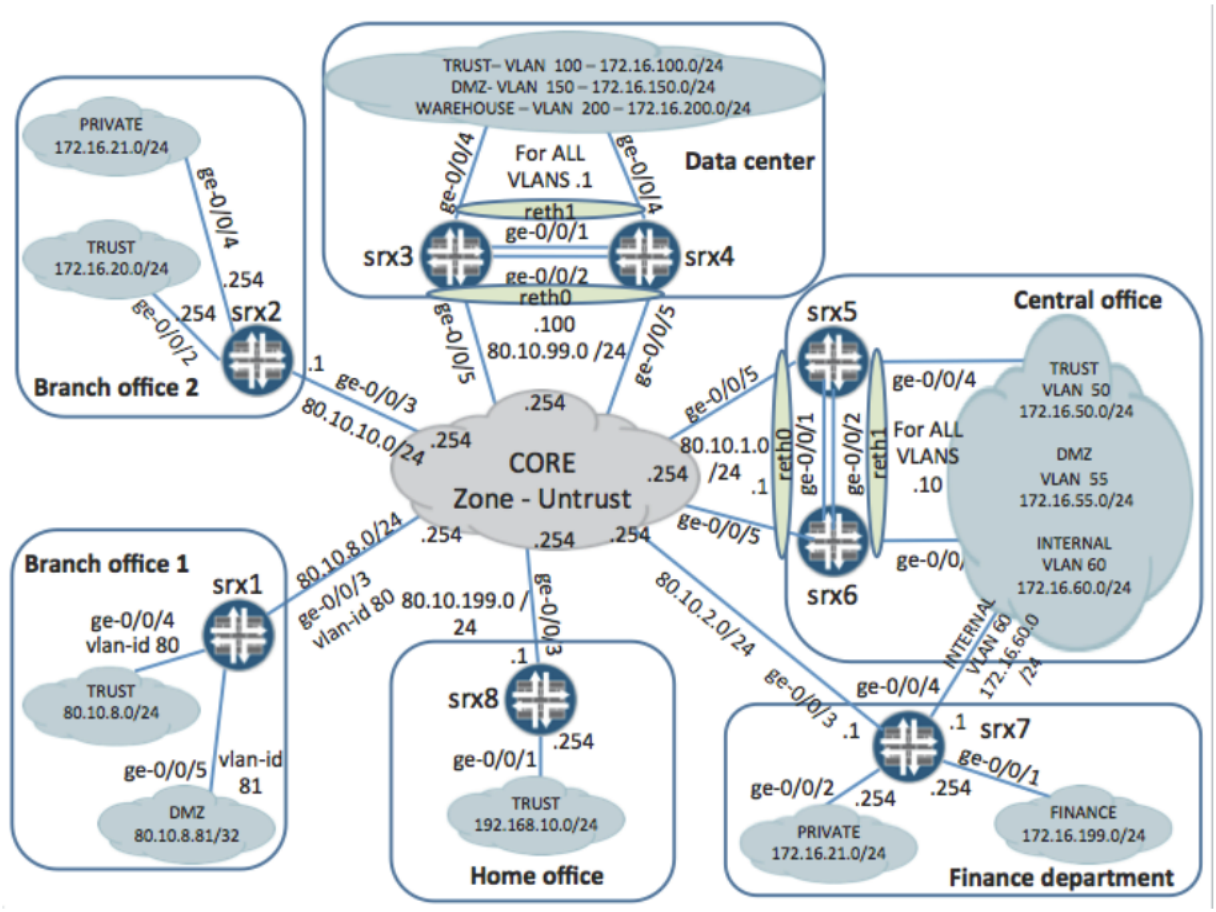
Another option for verification is traceoptions. The only flag available at the moment is "`all`".

```
[edit security idp traceoptions]
lab@cluster2# show
file idp_ts;
flag all;
```

Appendix - Chapter eight: Extended Implementation Concepts

This chapter is focused on two features of JUNOS Security kit: Transparent mode and Filter Based Forwarding. The presented scenarios require you to reconfigure security devices srx1 and srx7 according to picture below.

Topology for chapter eight:



Task 1: Transparent Mode

In this section you need to configure Home office's security device in such that srx1 will make forwarding decisions based on MAC address rather than on the base of IP header's information.

1) Configure the interfaces, bridge domain and security zones on the srx1 according to the table below, which reflects the topology image.
   Rewrite vlan-id 81 with the vlan-id 80 on the trunk port ge-0/0/5.0.

Interface	IP address	Interface mode	VLAN-ID	Zone
ge-0/0/4.0	N/a	Access	80	TRUST
ge-0/0/5.0	N/a	Trunk	81	DMZ
ge-0/0/3.0	N/a	Access	80	UNTRUST
irb.0	80.10.88.5/24		80	N/a

The main difference between configurations for transparent mode of operations and Layer 3 mode is the configuration of logical interfaces. You do not need to specify "`family inet`" and ip addresses any more. Instead of this "`family bridge`" must be associated with the logical units as well as interface mode (access or trunk) and vlan-id value regardless if Ethernet port is in the trunk or in the access mode.

The code excerpt below provides you with the example how interface configuration can be accomplished. Note that for trunk interface ge-0/0/5.0 vlan tagging rewriting is applied.

```
[edit interfaces]
lab@srx1# show
ge-0/0/4 {
    unit 0 {
        family bridge {
            interface-mode access;
            vlan-id 80;
        }
    }
}
ge-0/0/5 {
    vlan-tagging;
    unit 80 {
    family bridge {
    interface-mode trunk;
            vlan-id-list 80;
            vlan-rewrite {
                translate 81 80;
            }
        }
}
}
ge-0/0/6 {
    unit 0 {
    family bridge {
        interface-mode access;
            vlan-id 80;
        }
    }
}
irb {
     unit 0 {
         family inet {
             address 80.10.88.5/24;
         }
    }
}

[edit bridge-domains]
lab@srx1# show
vlan80 {
    domain-type bridge;
    vlan-id 80;
}
```

The security device will be converted into the transparent mode only after the system's reboot:

```
lab@srx1> request system reboot
```

Keep in mind that in current version of software you cannot use Junos security device both in layer 2 and in layer 3 modes.

The rest of configuration is similar to steps that are discussed in Chapter 3 "Firewall. Security policies".

NOTE: Unlike the ScreenOS transparent mode's configuration the security zone's layer of operations in JUNOS is determined by the configuration of interfaces that are bind to the particular security zone.

1) Configure static default route pointing to the IP address 80.10.8.1/24.
2) The hosts from the TRUST zone and its network range can go to the outside network (internet) with http and https.
3) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.
4) Devices in the DMZ zone should be accessible from the whole private corporate network including the local TRUST zone with https.
5) No other connections are allowed to go in or out of the TRUST zone.
6) No connections are allowed to go out from DMZ zone. Log all violations going out to the CORE network.
7) Ensure that irb.0 interface with IP address 80.10.8.5 is accessible with ping, telnet and http only from the TRUST zone.

Task 2: Filter Based Forwarding

In this section you need to configure Finance department's security device in such that srx7 will forward packets originated from PRIVATE and FINANCE zones on the based on criteria other then destination ip address.

There are two network paths to the Core network available in the Finance department. One path is direct connection to the Core network via interface ge-0/0/3.0. Another path leads to the Core network via the Central office network and is formed on the base of interface ge-0/0/4.60.

1) Configure srx7 in such that HTTPS traffic originated either from the PRIVATE or from the FINANCE zone and destined to the prefix 80.10.99.0/24 is forwarded via interface ge-0/0/3.0. All other traffic should be forwarded via interface ge-0/0/4.60
2) Ensure that asymmetric traffic forwarding is not possible.

The main goals of this task can be accomplished in three steps.

I. The first step assumes that ingress traffic needs to be classified according to the forwarding criteria. You will create firewall filters that should be applied as input filters to interfaces ge-0/0/1.0 and ge-0/0/2.0. The purpose of this firewall filters is to identify HTTP traffic and redirect it to the special routing instance which forwards packets differently from the muster routing instance.

```
[edit firewall family inet filter fbf term match-https]
lab@srx7# show
from {
    protocol tcp;
    port https
}
then {
    routing-instance fbf-instance;
}
```

As soon as firewall filter is created apply it to the interfaces ge-0/0/1.0 and ge-0/0/2.0 in input direction using commands below:

```
lab@srx7# set interface ge-0/0/1.0 family inet filter input fbf
lab@srx7# set interface ge-0/0/2.0 family inet filter input fbf
```

II. The goal of second step is to create such a routing instance which forwarding behavior will be different from the master routing instance inet.0. In simple words, we want to define different default gateway for https traffic.

```
[edit routing-instances fbf-instance]
lab@srx7# show
instance-type forwarding;
routing-options {
    static {
        route 0.0.0.0/0 next-hop 80.10.2.254;
    }
}
```

III. All interfaces direct routes are located in the master routing instance `inet.0`. It means that routing instance `fbf-instance` cannot resolve next-hop's ip address for the default route. Configuring rib-group element can solve this issue. The idea is to describe which routes must be copied from the `inet.0` into the `fbf-instance`. Here you are going:

```
[edit routing-options]
lab@srx7# show
interface-routes {
    rib-group inet int-routes;
}
rib-groups {
    int-routes {
        import-rib [ inet.0 fbf-instance.inet.0 ];
    }
}
```

The goal of step 6 can be accomplished by ensuring that source NAT is applied to traffic originated from the PRIVATE and FINANCE security zones.

Task 3: Verification

Transparent Mode

All commands that you learned in appendix for chapter 3 are applicable here as well.

It also can be useful to verify the status of security device's interfaces, in which mode they operate, to which bridge domains they belong.

```
lab@srx8> show interfaces
lab@srx8> show bridge domain
```

If you are satisfied with the interfaces and vlans configuration it is time to check the content of the bridge table with the command below.

```
lab@srx8> show bridge mac-table
```

Filter based forwarding.

First of all, initiate https session from either the PRIVATE or the FINANCE security zone. It can be done with the command below:

```
lab@srx7> telnet 172.31.10.1 port 443
```

Check session table of srx7 to ensure that https connection is established via the outgoing interface ge-0/0/2.0. Here is the command for this action:

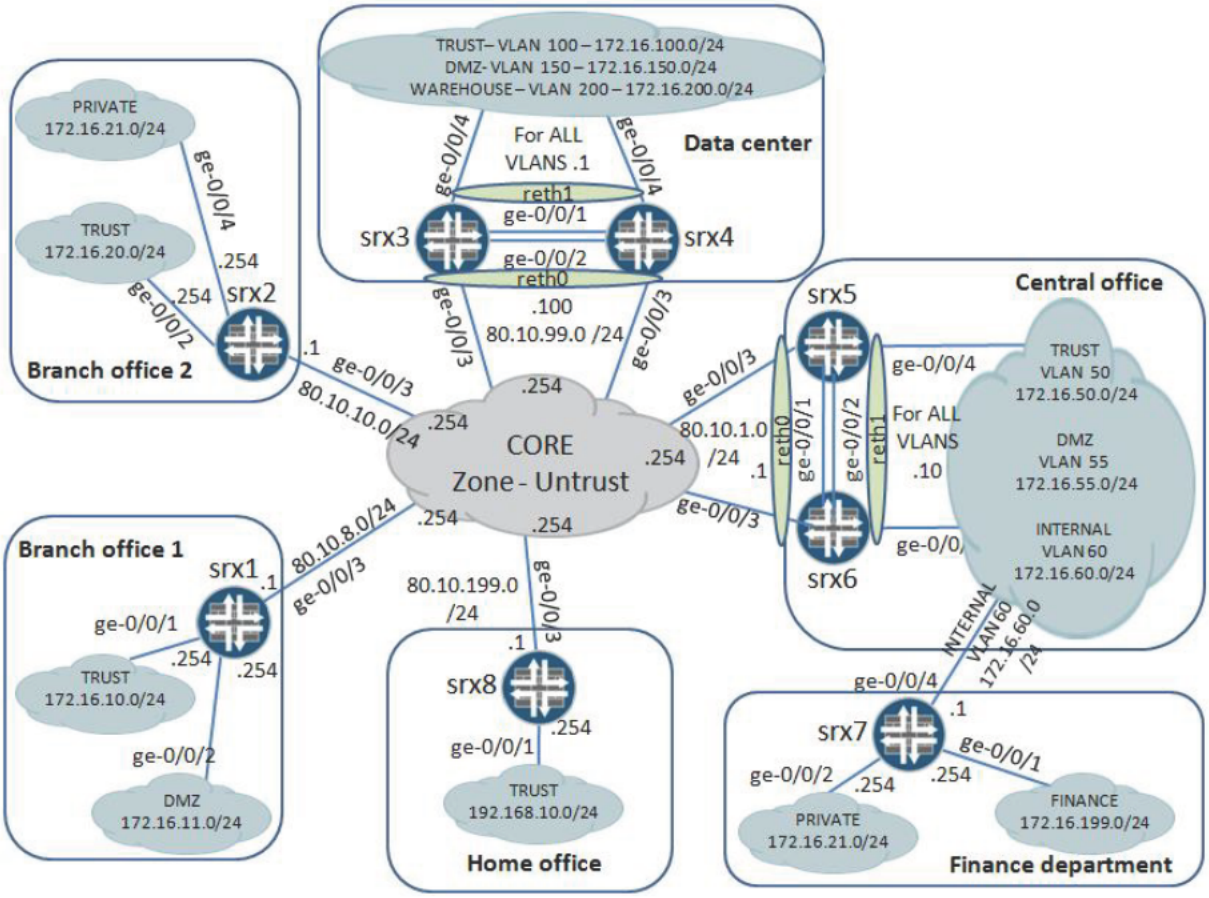
```
lab@srx7> show security flow session protocol tcp port 443
```

NOTE: If you failed to observe expected entries in the session table ensure that security policies from the PRIVATE and from the FINANCE zones to the UNTRUST zone exist and permit http traffic.

Appendix - Chapter nine: AppSecure

In this appendix section you will find the solutions for tasks from the AppSecure chapter. The configuration for all features (AppID, AppTrack, AppFW, AppQoS, SSL proxy and user-identification) is provided.

Topology for chapter nine:



Task 1: AppID

This task is about application identification (AppID).

Data center: cluster 1

5) The application system cache (ASC) configuration is located under [edit services application-identification] stanza. The cache timeout is defined with the command below. The parameter takes values in seconds: 2 hours = 7200 seconds.

```
{primary:node0}[edit services application-identification]
lab@srx3# set application-system-cache-timeout 7200
```

6) The following configuration excerpt enables the automatic AppID updates that start from 30 of March at 23:30 with the update interval of 24 hours. To fulfill the task requirement just define the date that represents the day on which you are completing the task.

```
{primary:node0}[edit services application-identification]
lab@srx3# show
download {
    automatic {
        start-time 03-30.23:30;
        interval 24;
    }
}
```

Task 2: AppTrack

The following information is about how to configure the application tracking on the cluster 1 to meet the given requirements.

Data center: cluster 1

1) The AppTrack feature is enabled on per security zone basis. Once defined for a zone the firewall will generate session tracking messages for connections in that zone. Junos allows adjusting the message creation settings such as when the 1^{s} for a session is created either directly when the application is identifier or after the defined interval elapses, and interval for periodic updates.
   Execute the following commands to have the firewall create the initial tracking message right when the application identification concludes and then send an update every 10 minutes.

```
{primary:node0}[edit]
lab@srx3# set security application-tracking first-update

{primary:node0}[edit]
lab@srx3# set security application-tracking session-update-interval
10
```

The AppTrack messages are syslog messages that are generated by the RT_FLOW (same as security policy logs). For specific identification the "APPTRACK" string can be used. The task demands the logs being kept together with the security policy logs. Check the current syslog configuration.

```
{primary:node0}[edit]
lab@srx3# show system syslog
user * {
    any emergency;
}
host 10.10.10.2 {
    any emergency;
    source-address 192.168.1.3;
}
file messages {
    any critical;
}
file interactive-commands {
    interactive-commands info;
}
file security-policy-logs {
    user info;
    match RT_FLOW;
    archive size 512k files 20;
}
file authorization-file {
    authorization info;
}
time-format year;
```

From the syslog configuration above (currently present on cluster 1) the security-policy-logs file will store the AppTrack messages right away.

Enable the AppTrack for the TRUST zone.

```
{primary:node0}[edit]
lab@srx3# set security zones security-zone TRUST application-
tracking
```

Task 3: AppFW

Here the details can be found about the configuration of the application firewall according to the posted tasks.

Data center: cluster 1

4) The AppFW configuration uses rule-set structure (similar as NAT configuration). The AppFW rule-sets can be defined in one of two ways:
   a. whitelist default rule's action is deny and other rules have the action of permit and list the allowed applications
   b. blacklist default rule's action is permit and other rules contain the action of deny and specify unwanted applications

   The task asks about blocking a specific application (junos:BITTORRENT) which is a clear case for blacklist.

```
{primary:node0}[edit security application-firewall]
lab@srx3# show
rule-sets deny-spec-APPS {
    rule deny-BT {
        match {
            dynamic-application junos:BITTORRENT;
        }
        then {
            deny;
        }
    }
    default-rule {
        permit;
    }
}
```

At last the defined AppFW rule set has to be referenced from a security policy permit action. The instructions specify that bittorrent has to be denied over the port 80 (junos-http predefined application matches on it) from the zone the TRUST to the zone UNTRUST. Because no such policy currently exists on the cluster 1 a new one has to be defined. The commands below create a new policy based on the given criteria and associate the AppFW rule-set with it:

```
{primary:node0}[edit]
lab@srx3# edit security policies from-zone TRUST to-zone UNTRUST

{primary:node0}[edit security policies from-zone TRUST to-zone
UNTRUST]
lab@srx3# set policy http-access match source-address trust-address-
range destination-address any application junos-http

{primary:node0}[edit security policies from-zone TRUST to-zone
UNTRUST]
lab@srx3# set policy http-access then permit application-services
application-firewall rule-set deny-spec-APPS
```

The new policy will be placed at the end of the list within the TRUST -> UNTRUST zone context. In order for it to be reached and used it has to be moved in front of the "internet-denied-log" policy (denies everything):

```
{primary:node0}[edit security policies from-zone TRUST to-zone
UNTRUST]
lab@srx3#  insert policy http-access before policy internet-denied-
log
```

A specific custom message "Bittorrent is BLOCKED!!!" has to be used for the denied sessions. Custom messages are defined in profiles under the [edit security application-firewall] stanza. These profiles in turn are referenced from AppFW rule-sets where the custom message should be applied. The next two commands define the required custom message and associate it with the new AppFW rule-set to accommodate the task requirements.

```
{primary:node0}[edit security application-firewall]
lab@srx3# set profile Bittorrent-message block-message type custom-
text content "Bittorrent is BLOCKED!!!"

{primary:node0}[edit security application-firewall]
lab@srx3# set rule-sets deny-spec-APPS profile Bittorrent-message
```

5) This task asks to allow only the junos:GMAIL and junos:GOOGLETALK applications in the connections over the port 80 from the DMZ to the UNTRUST zone. This time the rules-set will be a whitelist. For rule matching two options exist:

   a. list both applications in the rule match criteria

```
{primary:node0}[edit security application-firewall]
lab@srx3# show rule-sets allow-spec-APPS
rule allow-GOOGLE-apps {
    match {
        dynamic-application [ junos:GMAIL junos:GOOGLETALK ];
    }
    then {
        permit;
    }
}
default-rule {
    deny;
}
```

   b. create an application group that will contains both applications a use that group in the rule match criteria

```
{primary:node0}[edit services application-identification]
lab@srx3# show
...
application-group google-APPS {
    applications {
        junos:GMAIL;
        junos:GOOGLETALK;
    }
}
```

```
{primary:node0}[edit security application-firewall]
lab@srx3# show rule-sets allow-spec-APPS
rule-sets allow-spec-APPS {
    rule allow-GOOGLE-apps {
        match {
            dynamic-application-group google-APPS;
        }
        then {
            permit;
        }
    }
    default-rule {
        deny;
    }
}
```

A new security policy has to be created because the DMZ -> UNTRUST zone context is currently empty. The task mentions that connections over the port 443 have to be controlled. The predefined application junos-https is a good fit to be used in the security policy match criteria. This policy has to reference the new AppFW rule-set in the permit action.

```
{primary:node0}[edit security policies from-zone DMZ to-zone
UNTRUST]
lab@srx3# show
policy allow-specific-APPs {
    match {
        source-address [ co-dmz-range any ];
        destination-address any;
        application junos-https;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set allow-spec-APPS;
                }
            }
        }
    }
}
```

6) The firewall generates session deny messages only for policies that have logging with the "session-init" option enabled. The "session-close" option is not sufficient in this case because it creates only session close messages. Therefore to comply with the task the "session-init" logging has to be defined for both new security policies.

```
{primary:node0}[edit security policies]
lab@srx3# set from-zone TRUST to-zone UNTRUST policy http-access
then log session-init
```

```
{primary:node0}[edit security policies]
lab@srx3# set from-zone DMZ to-zone UNTRUST policy allow-specific-
APPs then log session-init
```

Task 4: AppQoS

In here the AppQoS configuration is listed that fulfills the given requirements.

Data center: cluster 1

2) The location of the AppQoS configuration is under the [edit class-of-service application-traffic-control] stanza. The main part is based on rule-sets (similar as AppFW) where the defined information tells what applications to look for and then how to handle them from the class of service perspective (e.g. apply rate limiters, change the priority bits and forwarding class). The last step referencing the rule-set within the security policy permit action might now come as no surprise.
   The AppQoS can use rate-limiters that are defined under the same hierarchy ([edit class-of-service application-traffic-control]) as the rule-sets.
   The task instructs to limit the junos:GMAIL application to the limit of 50000kb/s with burst of 312kB. Below is the rate-limiter configuration that reflects these values.

```
{primary:node0}[edit class-of-service]
lab@srx3# show
application-traffic-control {
    rate-limiters gmail-rl {
        bandwidth-limit 50000;
        burst-size-limit 312000;
    }
}
```

NOTE: Please keep in mind the bandwidth is defined in kilobits per second whereas the burst-size-limit is defined in bytes.

The rule-set accommodating the requirements (rate-limiting the junos:GMAIL application in the "from server" direction, setting the loss priority to high once the rate-limiter threshold is crossed and changing the dscp priority bits) follows:

```
{primary:node0}[edit class-of-service application-traffic-control]
lab@srx3# show rule-sets gmail-rs
rule-sets gmail-rs {
    rule gmail {
        match {
            application junos:GMAIL;
        }
        then {
            dscp-code-point ef;
            rate-limit {
                server-to-client gmail-rl;
                loss-priority-high;
            }
        }
    }
}
```

Traffic where this specific CoS behavior has to be enforced is from the DMZ to the UNTRUST zone. A security policy in the DMZ to UNTRUST zone context already exists (from task 3 AppFW). Only the reference to the AppQoS rule-set has to be added under the permit action.

```
{primary:node0}[edit]
lab@srx3# set security policies from-zone DMZ to-zone UNTRUST policy
allow-specific-APPs then permit application-services application-
traffic-control rule-set gmail-rs
```

The security policy then looks like this:

```
{primary:node0}[edit]
lab@srx3# show security policies from-zone DMZ to-zone UNTRUST
policy allow-specific-APPs
match {
    source-address dmz-range;
    destination-address any;
    application junos-https;
}
then {
    permit {
        application-services {
            application-firewall {
                rule-set allow-spec-APPS;
            }
            application-traffic-control {
                rule-set gmail-rs;
            }
        }
    }
    log {
        session-init;
    }
}
```

Task 5: SSL Proxy

This part handles the SSL Proxy configuration based on the given tasks.

Data center: cluster 1

1) First step is to locally generate the certificate for signing the modified server certificates that will be presented to the end user. The task contains details which the signing certificate must fulfill. The certificate creation requires a key to be present. So the starting point is the key generation with the given specifics:

```
{primary:node0}
lab@srx3> request security pki generate-key-pair certificate-id MY-
CERT size 1024 type rsa
```

Then the certificate generation follows:

```
{primary:node0}
lab@srx3> request security pki local-certificate generate-self-
signed certificate-id MY-CERT domain-name inetzero.com subject
"DC=IZ,CN=Inet-zero,OU=unit-1,O=inet-
zero,SN=1234,L=Amsterdam,ST=NL,C=NL" email jncie@inetzero.com add-
ca-constraint
```

NOTE: Please keep in mind the "add-ca-constraint" parameter is crucial here. It tells the device to generate a certificate for signing other certificates.

2) Due the nature of SSL proxy feature the end user gets a modified server certificate instead of the original one. That means he is not able to do the verification himself. This task is performed on the SRX by default (but can be disabled through configuration the "ignore-server-auth" action in the SSL proxy profile). However the SRX needs to know which CA certificates to use for the server certificate validation. A CA-profile-group is used for that. Below is the command that loads the CA certificate for validation from the file listed in the task.

NOTE: Please keep in mind in case the "ignore-server-auth" action is used this step is not needed and can be skipped.

```
{primary:node0}
lab@srx3> request security pki ca-certificate ca-profile-group load
ca-group-name MY-CA-GROUP filename /etc/certs/EngineeringCA.pem
```

3) The configuration allows defining URLs that should bypass the SSL proxy processing a whitelist. The whitelist references addresses or address-sets from the global address book.

NOTE: Please keep in mind that two ways are supported on SRXs for defining the addresses and address-sets:

- "Old" style the addresses and address-sets are defined in address-book under the security zone
- "New" style the address-books are defined right under [edit security] stanza and zones are attached to them. One address-book called "global" can be used by each security zone by default without any explicit association or attachment.

However, the configuration allows the use of only one of the styles at a time, i.e. they cannot be used together in the same configuration.

As mentioned above the SSL proxy whitelist uses the addresses/address-sets from the global address book. This means the "new" style has to be used in the configuration! If the configuration is using the "old" style it must be converted.

The task whitelist definition is below. Again two options exist group the addresses in an address-set or define multiple addresses directly in the whitelist parameter. The configuration below uses the address-set approach:

```
{primary:node0}[edit]
lab@srx3# show security address-book
global {
    address JNPR {
        dns-name www.juniper.net;
    }
    address INETZERO {
        dns-name www.inetzero.com;
    }
    address GMAIL {
        dns-name www.gmail.com;
    }
    address-set SSL-WHITELIST {
        address JNPR;
        address INETZERO;
        address GMAIL;
    }
}
```

NOTE: Please keep in mind the DNS server has to be configured (set system name-server A.B.C.D) when using domain names for the address entries. Otherwise the system will not be able to resolve them to IP addresses.

4) Now the SSL proxy profile needs to be configured (the configuration hierarchy is [edit services ssl proxy]). The SSL proxy profile contains details about the certificate to be used for signing the modified server certificates, which CA certificates to use for server authentication or disables the authentication, what to log and the whitelist.
The SSL proxy profile configuration below meets the task requirements.

```
{primary:node0}[edit]
lab@srx3# show services ssl
proxy {
    profile MY-SSL-PROFILE {
        trusted-ca MY-CA-GROUP;
        root-ca MY-CERT;
        whitelist SSL-WHITELIST;
        actions {
            log {
                sessions-allowed;
            }
        }
    }
}
```

In addition the task asks for sending the SSL proxy logs into the "ssl-proxy" file. The SSL proxy generates the log messages with the facility of PFE. The "match SSL" statement ensures that only SSL proxy generated messages go into the file and no other. Below is the syslog configuration excerpt.

```
{primary:node0}[edit]
lab@srx3# show system syslog file ssl-proxy
pfe any;
match SSL;
```

Finally the SSL proxy profile has to be referenced from the security policy permit action. Currently no suitable security policy exists from TRUST to UNTRUST zone that could be used for referencing the SSL proxy profile. Therefore a new one has to be created. The configuration is shown below:

```
policy https-traffic {
    match {
        source-address trust-address-range;
        destination-address any;
        application junos-https;
    }
    then {
        permit {
            application-services {
                ssl-proxy {
                    profile-name MY-SSL-PROFILE;
                }
            }
        }
    }
}
```

This new policy is placed at the end in the TRUST to UNTRUST zone context. To achieve correct operation it has to be moved in front of the "internet-denied-log" policy. The following command does just that:

```
{primary:node0}[edit security policies from-zone TRUST to-zone
UNTRUST]
lab@srx3# insert policy https-traffic before policy internet-denied-
log
```

The resulting security policies sequence in the TRUST to UNTRUST zone context:

```
{primary:node0}[edit security policies from-zone TRUST to-zone
UNTRUST]
lab@srx3# show | no-more
policy corp-access {
    match {
        source-address trust-address-range;
        destination-address corp-network;
        application any;
    }
    then {
        permit;
    }
}
policy http-access {
    match {
        source-address trust-address-range;
        destination-address any;
        application junos-http;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set deny-spec-APPS;
                }
            }
        }
        log {
            session-init;
        }
    }
}
policy https-traffic {
    match {
        source-address trust-address-range;
        destination-address any;
        application junos-https;
    }
    then {
        permit {
            application-services {
                ssl-proxy {
                    profile-name MY-SSL-PROFILE;
                }
```

```
                }
            }
        }
}
policy internet-denied-log {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        deny;
        log {
            session-init;
        }
    }
}
```

Task 6: User identification

This part provides insight into the solution for the user identification task that involves active directory.

Data center: cluster 1

2) The task is focused on the security policy matching criteria. It asks to enhance the typical thee parameters source address, destination address and application (ports and protocol number) with one more criterion user-identity. But the device needs to have information about users and their identity to be able to use this criterion. This information can be supplied from various sources:
    a. manually entered through CLI (called local)
    b. provided/retrieved from external sources (such as JPAC or Active Directory)
    c. the end users can be prompted for it (called firewall authentication)

   Sources can be combined and in such case the devices tries one after the other. The order in which the device uses individual sources depends on their priorities (the lower the better). The default sequence is: local (priority 100) -> active directory (priority 125) -> firewall authentication (priority 150) -> unified-access-control (priority 200).
   Here only the active directory is requested. Its priority should be set to 25.

```
{primary:node0}[edit]
lab@srx3# set security user-identification authentication-source
active-directory-authentication-table priority 25
```

Next the active directory details need to be configured so the firewall knows how to reach it. The following configuration excerpt uses the values from the task.

```
{primary:node0}[edit services user-identification]
lab@srx3# show
active-directory-access {
    domain jnciesec.inetzero.com {
        user {
            administrator;
            password "$9$Yp4JUF39pu1qmz69Cu0Lx7V24"; ## SECRET-DATA
        }
        domain-controller AD-server {
            address 10.10.10.10;
        }
        user-group-mapping {
            ldap {
                base DC=jnciesec,DC=inetzero,DC=com;
            }
        }
    }
}
```

The final step is to include the "user-identity" parameter in the matching criteria of the appropriate security policy. The task defines to use the "jncie-sec-exam" value for this parameter in the security policy that handles the access from the TRUST zone to the corporate network (zone UNTRUST). By examining the current policies in this context (TRUST to UNTRUST) the policy "corp-access" looks like to perfect candidate because of its criteria source address matches the TRUST subnet and destination address matches the corporate subnet. The resulting policy configuration is displayed below:

```
{primary:node0}[edit security policies from-zone TRUST to-zone
UNTRUST]
lab@srx3# show policy corp-access
match {
    source-address trust-address-range;
    destination-address corp-network;
    application any;
    source-identity jncie-sec-exam;
}
then {
    permit;
}
```

In case no good fit can be found in the existing policies a new one has to be created and placed on the correct spot.