LOMBA KOMPETENSI SISWA

SEKOLAH MENENGAH KEJURUAN

TINGKAT NASIONAL XXVIII 2020

TEST PROJECT

IT NETWORK SYSTEMS ADMINISTRATION

LKS2020_NETWORK_Actual

Basic configuration

1. Configure hostnames for ALL devices according to the topology.
2. Configure domain name **lksn2020.id** for ALL network devices on the topology.
3. Create user **lksn2020** on ALL devices.

   (a) Remote and local console authentication should use local username database.

   (b) After successful authentication user should automatically land in privileged mode (level 15)

4. Configure privileged mode access on **FW-01** and **TOF** using username's password. Example username **nusantara** with password **indonesia** should be able to enter privileged mode with password **indonesia.**
5. Create all necessary interfaces, subinterfaces and SVIs on ALL devices. Use IP addressing according to the table below.

Device	Interface	IP address
MOW	Gi0/1	132.87.2.100/24
	Loopback 100	192.168.254.1/30
KVX	Gi0/1	94.121.72.18/24
	Loopback 200	192.168.30.254/24
YKS	Gi0/1	18.31.192.12/24
	Loopback 300	192.168.40.254/24
FW-01	G0/1	192.168.254.2/30
	Vlan 10	192.168.10.254/24
	Vlan 20	192.168.20.254/24
DSW-01	Vlan 10	192.168.10.11/24
DSW-02	Vlan 20	192.168.20.12/24
RTK	Gi1/0/1	100.10.9.6/30
	Gi0/5	94.121.72.96/24

	Gi0/4	132.87.2.1/24
	Gi0/2	100.71.60.254/29
	Gi0/3	18.31.192.71/24
	Loopback 700	172.40.20.254/24
	Loopback 800	193.166.9.254/24
TOF	Gi0/1	100.10.9.5/30
	Loopback 400	172.16.100.254/24
TJM-01	Gi0/1	100.71.60.252/29
	Loopback 500	172.20.0.251/24
TJM-02	Gi0/1	100.71.60.251/29
	Loopback 600	172.20.0.252/24

HQ and Branch LAN

1. Create VLANs on DSW-01 and DSW-02, assign names and ports according to the topology diagram. When adding any new VLAN to DSW-01, this VLAN should be automatically distributed to DSW-02.
2. DSW-01 should initiate trunk negotiation via DTP and be STP root in ALL VLANs. Use non-default STP protocol. Make necessary configuration to prevent STP root change attacks.
3. Configure link aggregation between DSW-01 and DSW-02. Use any LAG protocol.
4. Make sure that end user devices are not waiting for STP recalculation when plugged into the network.
5. Configure DHCP scopes on Moscow, Kazan, Tyumen, Yakutsk and Sakhalin sites.
6. Ensure protection from DHCP attacks as well as from ARP-spoofing attacks on Moscow site.

Public Internet

1. Configure internet routing domain according to the topology diagram. Use BGP with AS numbers from 65000-65005

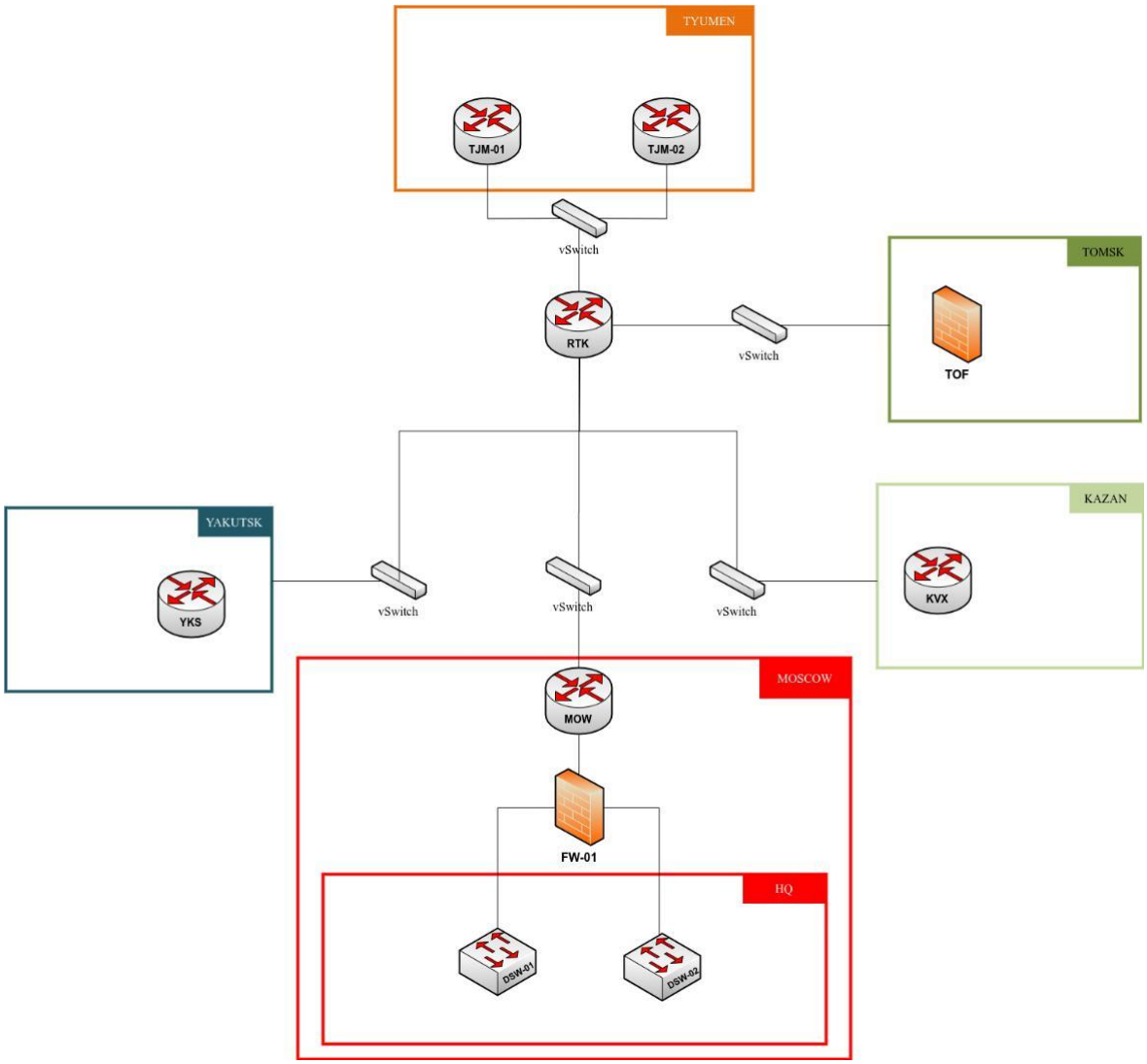
Enterprise Routing

1. Configure enterprise routing domain according to the topology diagram. Use any dynamic routing protocol.
2. All traffic must be encrypted with IPsec while traversing via public internet.
3. Ensure end-to-end connectivity between all end user virtual machines inside enterprise routing domain.

Advanced Configuration

1. Synchronize time on all network equipment using NTP (time zone WITA +8). Use **RTK** as the root NTP server. Configure hierarchical NTP infrastructure use **MOW** as a corporate NTP server.
2. Enable SSH on all network devices and implement local user **lksn2020** with password **Passw0rd$** with privilege level 15 (use only for VTY lines). Make sure SSH is accessible via anywhere.
3. Configure role-based access control on RTK router:
   (a) Create **user1**, **user2**, **user3**, **user4** and **user5** with **cisco1** password.
      i. **user1** should be authorized to issue all privileged mode commands except "**show version**" and "**show ip route**" but should be able to issue "**show ip ***" commands.
      ii. **user2** should be authorized to issue all user (unprivileged) mode commands including "**show version**" but not "**show ip route**".
   (b) Create view-context "**show_view**":
      i. Include "**show version**" command
      ii. Include all unprivileged commands of "**show ip ***"
      iii. Include "**who**" command
      iv. **user3** should land in this context after successful authentication on local or remote console.
   (c) Create view-context "**ping_view**":
      i. Include "**ping**" command
      ii. Include "**traceroute**" command
      iii. **user4** should land in this context after successful authentication on local or remote console.
   (d) Create superview-context that combines these 2 contexts. **user5** should land in this superview-context after successful authentication on local or remote console.
   (e) Make sure that users cannot issue any other commands within contexts that are assigned to them (except show banner and show parser, which are implicitly included in any view).
4. TJM-02 should act as stateless failover for all traffic from Tyumen towards the internet and enterprise routing domain and vice versa. In case of TJM-01 failure TJM-02 should take over all roles of TJM-01 so all network services will continue normal operation.
5. Implement necessary security measures on MOW site border to expose minimum services towards public internet.

Topology


TYUMEN
TJM-01
TJM-02
vSwitch
TOMSK
RTK
vSwitch
TOF
YAKUTSK
YKS
vSwitch
vSwitch
vSwitch
KAZAN
KVX
MOSCOW
MOW
FW-01
HQ
DSW-01
DSW-02

Routing Diagram