#!/usr/bin/clish

#20

#1.14.1

#02/11/2021

#14:43:21

hostname esr-10

object-group service ssh

 port-range 22

exit

object-group service dhcp\_server

 port-range 67

exit

object-group service dhcp\_client

 port-range 68

exit

object-group service ntp

 port-range 14

exit

object-group network Subnet\_Camera

 ip prefix 10.98.234.128/26

exit

object-group network Subnet\_Cloud

 ip prefix 10.16.130.0/23

exit

object-group network Subnet\_FMPM

 ip prefix 10.0.211.64/26

 ip prefix 10.0.227.32/27

 ip prefix 10.100.0.64/27

 ip prefix 10.0.220.64/27

 ip prefix 10.100.0.224/29

 ip prefix 10.0.230.128/25

 ip prefix 10.16.130.0/23

 ip prefix 10.0.236.32/27

exit

object-group network Subnet\_Controller

 ip prefix 10.0.235.32/27

 ip prefix 10.0.234.32/27

 ip prefix 10.154.10.128/29 - существующий softwlc (ЦОД ПНО). Он будет один на все объекты, этот адрес не меняем

exit

object-group network Subnet\_Mgmt

 ip prefix 10.12.234.128/26

 ip prefix 10.159.123.0/24 – NAT, подсеть берем из столбца AD

exit

object-group network Local\_Subnet

 ip prefix 10.135.84.0/23

 ip prefix 10.154.191.0/24

 ip prefix 10.156.123.0/24 - ESR20, подсеть берем из столбца Z

 ip prefix 10.157.123.0/24 - ESR20, подсеть берем из столбца AA

 ip prefix 10.158.123.0/24 - ESR20, подсеть берем из столбца AB

exit

object-group network bgp\_export

 ip prefix 10.135.84.0/23

 ip prefix 10.98.234.128/26

 ip prefix 10.154.191.0/24

 ip prefix 10.12.234.128/26

 ip prefix 10.156.123.0/24 - ESR20, подсеть берем из столбца Z

 ip prefix 10.157.123.0/24 - ESR20, подсеть берем из столбца AA

 ip prefix 10.158.123.0/24 - ESR20, подсеть берем из столбца AB

 ip prefix 10.159.123.0/24 – ESR20 NAT, подсеть берем из столбца AD

 ip prefix 10.7.17.128/25 - ESR20, подсеть берем из столбца AC

exit

object-group network HW\_VipNET

 ip prefix 10.7.17.128/25 - ESR20, подсеть берем из столбца AC

exit

object-group network ex\_mgmt\_preCOS – платформенная часть существуюих сетей видеонаблюдения (ЦОД ПНО). Адреса эти едины для всех объектов, не меняем

 ip prefix 10.0.26.128/25

 ip prefix 10.0.44.0/24

exit

vlan 2

 name "Camera"

exit

vlan 3

 name "MGMT"

 force-up

exit

vlan 4

 name "LAN\_DHCP"

exit

security zone CAMERA

exit

security zone MGMT

exit

security zone LAN\_DHCP

exit

security zone WAN

exit

route-map from\_GPE

 rule 10

 match ip address 0.0.0.0/0

 action permit

 exit

 rule 20

 action deny

 exit

exit

route-map to\_GPE

 rule 10

 match ip address object-group bgp\_export

 action permit

 exit

 rule 20

 action deny

 exit

exit

router bgp 65000

 router-id 10.1.131.138

 neighbor 10.1.131.137

 description "CRYPTO\_IPC10"

 remote-as 65000

 update-source 10.1.131.138

 address-family ipv4 unicast

 route-map from\_GPE in

 route-map to\_GPE out

 next-hop-self

 enable

 exit

 enable

 exit

 address-family ipv4 unicast

 network 10.154.191.0/24

 network 10.12.234.128/26

 network 10.135.84.0/23

 network 10.98.234.128/26

 network 10.156.123.0/24 - ESR20, подсеть берем из столбца Z

 network 10.157.123.0/24 - ESR20, подсеть берем из столбца AA

 network 10.158.123.0/24 - ESR20, подсеть берем из столбца AB

 network 10.159.123.0/24 – ESR20 NAT, подсеть берем из столбца AD

 network 10.7.17.128/25 - ESR20, подсеть берем из столбца AC

 exit

 enable

exit

snmp-server

snmp-server community "yoe3nguPr@gc" ro client-list Subnet\_FMPM

snmp-server enable traps config

snmp-server enable traps config commit

snmp-server enable traps config confirm

snmp-server enable traps environment

snmp-server enable traps environment memory-flash-critical-low

snmp-server enable traps environment memory-flash-low

snmp-server enable traps environment memory-ram-critical-low

snmp-server enable traps environment memory-ram-low

snmp-server enable traps environment cpu-load

snmp-server enable traps environment cpu-critical-temp

snmp-server enable traps environment cpu-overheat-temp

snmp-server enable traps environment cpu-supercooling-temp

snmp-server enable traps file-operations

snmp-server enable traps file-operations successful

snmp-server enable traps file-operations failed

snmp-server enable traps file-operations canceled

snmp-server enable traps interfaces

snmp-server enable traps interfaces rx-utilization-high

snmp-server enable traps interfaces tx-utilization-high

snmp-server enable traps interfaces number-high

snmp-server enable traps screen

snmp-server enable traps screen dest-limit

snmp-server enable traps screen source-limit

snmp-server enable traps screen icmp-threshold

snmp-server enable traps screen udp-threshold

snmp-server enable traps screen syn-flood

snmp-server enable traps screen land

snmp-server enable traps screen winnuke

snmp-server enable traps screen icmp-frag

snmp-server enable traps screen udp-frag

snmp-server enable traps screen icmp-large

snmp-server enable traps screen syn-frag

snmp-server enable traps screen unknown-proto

snmp-server enable traps screen ip-frag

snmp-server enable traps screen port-scan

snmp-server enable traps screen ip-sweep

snmp-server enable traps screen syn-fin

snmp-server enable traps screen fin-no-ack

snmp-server enable traps screen no-flag

snmp-server enable traps screen spoofing

snmp-server enable traps screen reserved

snmp-server enable traps screen quench

snmp-server enable traps screen echo-request

snmp-server enable traps screen time-exceeded

snmp-server enable traps screen unreachable

snmp-server enable traps screen tcp-all-flags

snmp-server enable traps entity

snmp-server enable traps entity config-change

snmp-server enable traps entity-sensor

snmp-server enable traps entity-sensor threshold

snmp-server enable traps envmon

snmp-server enable traps envmon shutdown

snmp-server enable traps envmon temperature

snmp-server enable traps flash

snmp-server enable traps flash insertion

snmp-server enable traps flash removal

snmp-server enable traps snmp

snmp-server enable traps snmp authentication

snmp-server enable traps snmp coldstart

snmp-server enable traps snmp linkdown

snmp-server enable traps snmp linkup

snmp-server enable traps syslog

bridge 2

 description "CAMERA"

 vlan 2

 security-zone CAMERA

 ip address 10.98.234.129/26

 enable

exit

bridge 3

 description "MGMT"

 vlan 3

 security-zone MGMT

 ip address 10.12.234.129/26

 enable

exit

bridge 4

 description "LAN\_DHCP"

 vlan 4

 security-zone LAN\_DHCP

 ip address 10.135.84.1/23

 ip address 10.154.191.1/24

 enable

exit

interface gigabitethernet 1/0/1

 description "ESR20"

 mode switchport

 switchport access vlan 4

 lldp transmit

 lldp receive

exit

interface gigabitethernet 1/0/2

 description "KDPOE2"

 mode switchport

 switchport forbidden default-vlan

 switchport mode trunk

 switchport trunk allowed vlan add 2-4

 lldp transmit

 lldp receive

exit

interface gigabitethernet 1/0/3

 description "KDPOE3"

 mode switchport

 switchport forbidden default-vlan

 switchport mode trunk

 switchport trunk allowed vlan add 2-4

 lldp transmit

 lldp receive

exit

interface gigabitethernet 1/0/5

 description "KDPOE4"

 mode switchport

 switchport forbidden default-vlan

 switchport mode trunk

 switchport trunk allowed vlan add 2-4

 lldp transmit

 lldp receive

exit

interface gigabitethernet 1/0/6

 description "KDPOE5"

 mode switchport

 switchport forbidden default-vlan

 switchport mode trunk

 switchport trunk allowed vlan add 2-4

 lldp transmit

 lldp receive

exit

interface gigabitethernet 1/0/4

 description "WAN"

 security-zone WAN

 ip address 10.1.131.138/30

 lldp transmit

 lldp receive

exit

security zone-pair WAN self

 rule 10

 action permit

 match protocol tcp

 match source-address Subnet\_FMPM

 match destination-port ssh

 enable

 exit

 rule 30

 action permit

 match protocol icmp

 enable

 exit

 rule 40

 action permit

 match protocol udp

 match destination-port ntp

 enable

 exit

exit

security zone-pair LAN\_DHCP self

 rule 10

 action permit

 match protocol udp

 match source-port dhcp\_client

 match destination-port dhcp\_server

 enable

 exit

exit

security zone-pair WAN CAMERA

 rule 10

 action permit

 match source-address Subnet\_Mgmt

 match destination-address Subnet\_Camera

 enable

 exit

 rule 20

 action permit

 match source-address Subnet\_FMPM

 match destination-address Subnet\_Camera

 enable

 exit

exit

security zone-pair LAN\_DHCP WAN

 rule 10

 action permit

 enable

 exit

exit

security zone-pair LAN\_DHCP LAN\_DHCP

 rule 10

 action permit

 enable

 exit

exit

security zone-pair MGMT self

 rule 10

 action permit

 enable

 exit

exit

security zone-pair MGMT CAMERA

 rule 10

 action permit

 enable

 exit

exit

security zone-pair WAN MGMT

 rule 10

 action permit

 enable

 exit

exit

security zone-pair MGMT WAN

 rule 10

 action permit

 enable

 exit

exit

security zone-pair WAN LAN\_DHCP

 rule 10

 action permit

 match protocol gre

 enable

 exit

 rule 20

 action permit

 match destination-address HW\_VipNET

 enable

 exit

 rule 30

 action permit

 match source-address ex\_mgmt\_preCOS

 match destination-address HW\_VipNET

 enable

 exit

 rule 40

 action permit

 match source-address Subnet\_Controller

 match destination-address Subnet\_Mgmt

 enable

 exit

exit

ip dhcp-server

ip dhcp-server pool LAN\_DHCP

 network 10.135.84.0/23

 address-range 10.135.84.2-10.135.85.254

 default-router 10.135.84.1

 dns-server 95.167.167.96,95.167.167.95

exit

ip route 10.7.17.128/25 - ESR20, подсеть берем из столбца AC 10.154.191.254 – берем 254 адрес из подсети открытого сегмента (СКУП/IP план)колонка V

ip route 10.156.123.0/24 - ESR20, подсеть берем из столбца Z 10.154.191.254 – см.выше

ip route 10.157.123.0/24 - ESR20, подсеть берем из столбца AA 10.154.191.254 – см.выше

ip route 10.158.123.0/24 - ESR20, подсеть берем из столбца AB 10.154.191.254 – см.выше

ip route 10.159.123.0/24 – ESR20 NAT, подсеть берем из столбца AD 10.154.191.254 – см.выше

ip telnet server

ip ssh server

lldp enable

ntp enable

ntp broadcast-client enable

username admin

 password encrypted $6$Srrt7Bi0arsmeohw$TJTBWhSHYFEBI7DYbhwyHqDl94jEUCdwyXFYVKlw.0He1kGkoeq33GYv.Atf1njv2l76u5Bm6O2GmTb7ZKjta/

exit