version 12.4

service timestamps debug datetime msec (Se introduce en vyatta debug,

service timestamps log datetime msec warning e info)

no service password-encryption

service sequence-numbers (introduce nº’s en la secuencia de logs)

!

hostname Cisco2851Ats (Se cambia por Artigas en el Vyatta)

!

boot-start-marker (No aplica en config. Propietario Cisco)

boot-end-marker (No aplica en config. Propietario Cisco)

!

logging buffered 51200 warnings

logging console informational

no logging monitor (Configurado en Vyatta a través de Syslog)

!

no aaa new-model

clock timezone BsAs -2 (Se configura en Vyatta la zona)

!

!

ip cef (Protocolo de Cisco, no aplica en Vyatta)

!

!

ip domain name ba-02-ats.tpp.com.ar (Se configura en Vyatta)

ip name-server 200.69.193.1 (Se configura en Vyatta)

ip name-server 200.69.193.2 (Se configura en Vyatta)

!

!

!

username admtpp privilege 15 secret 5 $1$S8Qz$xKwIwQrS3bYoCAkrOwTi9. (User root y vyatta en Vyatta Artigas)

!

!

!

class-map match-all VOIP

match protocol rtp

match access-group name GATEWAY

class-map match-all SPFClass

match access-group name SPFNet

class-map match-all test

class-map match-any TEST

class-map match-any TRAFICO-GESTION

match protocol telnet

match protocol snmp

class-map match-all Test

class-map match-any TRAFICO-NORMAL-CLIENTES

match protocol pop3

match protocol http

match protocol imap

match protocol smtp

match protocol ftp

class-map match-any TRAFICO-P2P

match protocol edonkey

match protocol kazaa2

match protocol fasttrack

match protocol gnutella

match protocol pad

class-map match-any VOIP-CONTROL

match protocol h323

match protocol sip

match protocol mgcp

match protocol rtcp

!

!

policy-map TPP-OUT

class VOIP

priority 512

q class TRAFICO-P2P

shape average 378000 378000 378000

class class-default

fair-queue

shape average 1024000 1024000 1024000

policy-map SPF

class SPFClass

shape average 8000 1000 1000

!

(Se aplicó la política de QOS del Vyatta "traffic-policy random-detect", que es un mecanismo de prevención de la congestión, mecanismo que incluye Random Early Detection (RED), y Weighted Random Detección Temprana (WRED).  
Las congestiones de tráfico son causadas por la resincronización global de los equipos TCP, éstos al “hablar” reducen sus tasas de transmisión para tratar de despejar la congestión, lo que puede afectar significativamente el rendimiento de la red. Como despeja la congestión, la red aumenta las tasas de transmisión de nuevo hasta el punto en el que se vuelve a producir congestión. Este ciclo de congestión y compensación no hace el mejor uso del ancho de banda disponible.  
RED reduce la posibilidad de que la congestión de la red se produzca por la caída al azar de   
paquetes cuando la interfaz de salida comienza a mostrar signos de congestión. Éste sistema reduce la posibilidad global de sincronización, haciendo un mejor uso del ancho de banda de red.)

!

!

interface Tunnel1 (No está en uso)

no ip address

shutdown

!

interface GigabitEthernet0/0 (eth 0 nuevo Vyatta)

description "Iplan Internet-port 1 sw Iplan"

ip address 200.68.72.101 255.255.255.248

ip nat outside (duda)

ip route-cache flow

load-interval 30

duplex auto

speed auto

!

interface GigabitEthernet0/1 (eth 1 nuevo Vyatta)

description "TLS Viamonte-port 20 sw Iplan"

ip address 172.18.18.2 255.255.255.252

ip mask-reply

ip directed-broadcast

ip nat inside (duda)

ip route-cache flow

load-interval 30

duplex auto

speed auto

!

interface FastEthernet0/1/0 (eth 4 nuevo Vyatta)

description "UMG8900-OMC-slot 1-MNG"

switchport access vlan 4

duplex full

speed 100

!

interface FastEthernet0/1/1

description "DNS eth1"

switchport access vlan 4

shutdown

duplex full

speed 100

!

interface FastEthernet0/1/2 (eth 3 nuevo Vyatta)

description "Sw Penales port 1"

switchport access vlan 4

!

interface FastEthernet0/1/3 (eth 2 nuevo Vyatta)

description "DNS-10.77.128.2-eth2"

switchport access vlan 7

duplex full

speed 100

!

interface FastEthernet0/1/4 (No está conectada)

switchport access vlan 4

duplex full

speed 100

!

interface FastEthernet0/1/5 (eth 5 nuevo Vyatta)

description "UMG8900-FE0-Slot 3"

switchport access vlan 3

!

interface FastEthernet0/1/6 (eth 6 nuevo Vyatta)

description "UMG8900-VPU-FE0-RTP-Slot 1"

switchport access vlan 3

!

interface FastEthernet0/1/7 (eth 7 nuevo Vyatta)

description "Mux G. Catan-interface bridge"

switchport access vlan 4

!

interface FastEthernet0/1/8 (eth 8 nuevo Vyatta)

description "Mux San Martin-interface bridge"

switchport access vlan 4

!

interface Vlan1

no ip address

shutdown

!

interface Vlan3

description LinkUMG

ip address 201.216.254.97 255.255.255.248

ip mask-reply

ip directed-broadcast

ip route-cache flow

!

interface Vlan4

description LinkVia

ip address 10.10.129.1 255.255.255.240 secondary

ip address 10.44.128.1 255.255.255.0 secondary

ip address 10.10.127.1 255.255.255.0

ip mask-reply

ip directed-broadcast

ip nat inside (revisar)

ip route-cache flow

load-interval 30

!

interface Vlan7

description DNS

ip address 201.216.254.105 255.255.255.248 secondary

ip address 10.77.128.1 255.255.255.0

ip mask-reply

ip directed-broadcast

ip nat inside (revisar)

!

ip route 0.0.0.0 0.0.0.0 200.68.72.102

ip route 10.8.10.0 255.255.255.0 172.18.18.1

ip route 10.10.0.0 255.255.255.0 172.18.18.1

ip route 10.10.1.192 255.255.255.224 172.18.18.1

ip route 10.10.128.0 255.255.128.0 172.18.18.1

ip route 10.11.128.0 255.255.224.0 172.18.18.1

ip route 10.12.128.0 255.255.224.0 10.10.0.1

ip route 10.15.128.0 255.255.224.0 172.18.18.1

ip route 10.16.128.0 255.255.224.0 10.10.255.254

ip route 10.16.128.0 255.255.224.0 10.10.128.90

ip route 10.24.128.0 255.255.255.0 10.10.128.90

ip route 10.25.0.0 255.255.255.0 172.18.18.1

ip route 10.26.0.0 255.255.255.0 172.18.18.1

ip route 10.30.0.0 255.255.252.0 172.18.18.1

ip route 10.44.128.0 255.255.255.0 172.18.18.1

ip route 172.16.0.0 255.255.0.0 172.18.18.1

ip route 190.2.46.192 255.255.255.248 172.18.18.1

ip route 190.2.46.200 255.255.255.252 10.10.127.131

ip route 190.2.46.204 255.255.255.252 10.10.127.132

ip route 190.2.46.208 255.255.255.252 10.10.127.193

ip route 190.2.46.212 255.255.255.252 10.10.127.137

ip route 190.2.46.216 255.255.255.252 10.10.127.138

ip route 190.2.46.220 255.255.255.252 10.10.127.117

ip route 190.2.46.240 255.255.255.240 172.18.18.1

ip route 190.12.101.143 255.255.255.255 172.18.18.1

ip route 190.12.101.144 255.255.255.255 172.18.18.1

ip route 192.168.0.0 255.255.128.0 172.18.18.1

ip route 200.73.185.64 255.255.255.224 172.18.18.1

ip flow-export source Vlan4 (No está en uso el Netflow)

ip flow-export version 5

ip flow-export destination 10.10.128.128 9996

ip flow-top-talkers

top 10

sort-by bytes

match class-map TRAFICO-GESTION

!

ip http server (No, está en deshuso)

ip http access-class 1

ip http authentication local

no ip http secure-server

ip http timeout-policy idle 5 life 86400 requests 10000

ip nat pool Net1 200.68.72.100 200.68.72.101 netmask 255.255.255.248

ip nat inside source list 3 interface GigabitEthernet0/0 overload

ip nat inside source list 4 interface GigabitEthernet0/0 overload

ip nat inside source list 7 interface GigabitEthernet0/0 overload

ip nat inside source list 8 interface GigabitEthernet0/0 overload

ip nat inside source static tcp 10.10.128.248 3389 200.68.72.99 3389 extendable (se cambia 200.68.72.99 x 200.68.72.101, ya que al no estar en su rango el vyatta no toma la .99)

ip nat inside source static tcp 10.10.128.4 5948 200.68.72.99 5948 extendable (se cambia 200.68.72.99 x 200.68.72.101, ya que al no estar en su rango el vyatta no toma la .99)

ip nat inside source static tcp 10.10.128.212 5847 200.68.72.99 6847 extendable (se cambia 200.68.72.99 x 200.68.72.101, ya que al no estar en su rango el vyatta no toma la .99)

ip nat inside source static tcp 10.10.128.212 5947 200.68.72.99 6947 extendable (se cambia 200.68.72.99 x 200.68.72.101, ya que al no estar en su rango el vyatta no toma la .99)

ip nat inside source static tcp 10.10.1.200 5900 200.68.72.99 6948 extendable (se cambia 200.68.72.99 x 200.68.72.101, ya que al no estar en su rango el vyatta no toma la .99)

ip nat inside source static tcp 10.10.128.212 8080 200.68.72.99 8888 extendable (se cambia 200.68.72.99 x 200.68.72.101, ya que al no estar en su rango el vyatta no toma la .99)

ip nat inside source static tcp 10.10.128.128 8080 200.68.72.101 8888 extendable

!

ip access-list extended GATEWAY

permit ip host 200.73.184.142 any

permit ip any host 200.73.184.142

ip access-list extended SPFNet

permit ip 10.10.129.0 0.0.0.15 any

permit ip any 10.10.129.0 0.0.0.15

!

no logging trap

access-list 1 permit 190.30.233.2 (No parecen estar asociadas a ninguna interfaz)

access-list 1 permit 10.10.128.210

access-list 1 permit 10.10.128.211

access-list 1 permit 10.10.128.212

access-list 1 remark SDM\_ACL Category=2

access-list 1 permit 10.10.127.0 0.0.0.255

access-list 2 remark SDM\_ACL Category=2

access-list 2 permit 10.10.127.0 0.0.0.255

access-list 3 remark SDM\_ACL Category=2

access-list 3 permit 10.10.128.0 0.0.127.255

access-list 3 permit 172.16.1.0 0.0.0.255

access-list 3 permit 10.44.128.0 0.0.0.255 (en deshuso)

access-list 4 permit 10.12.128.0 0.0.0.15

access-list 5 remark SDM\_ACL Category=2

access-list 5 permit 10.25.0.0 0.0.0.255

access-list 5 permit 10.26.0.0 0.0.0.255

access-list 6 remark SDM\_ACL Category=2 (No parecen estar asociadas a ninguna interfaz)

access-list 6 permit 190.12.101.143

access-list 6 permit 190.12.101.142

access-list 6 permit 190.12.101.141

access-list 6 permit 10.12.0.0 0.0.0.15

access-list 7 remark SDM\_ACL Category=2

access-list 7 permit 192.168.0.0 0.0.127.255

access-list 8 remark SDM\_ACL Category=2

access-list 8 permit 10.10.127.117

access-list 8 permit 10.10.127.233

access-list 8 permit 10.10.127.193

access-list 8 permit 10.77.128.5

access-list 8 permit 10.77.128.4

access-list 8 permit 10.77.128.3

access-list 8 permit 10.77.128.2

access-list 8 permit 10.77.128.1

access-list 8 permit 10.10.127.144

access-list 8 permit 10.10.127.132

access-list 30 permit 190.14.171.0 0.0.0.127 (No parecen estar asociadas a ninguna interfaz)

access-list 130 deny ip host 201.216.254.11 any

access-list 130 deny ip any host 201.216.254.11

access-list 130 permit ip any any

access-list 130 remark PosibleIpCamHdSol

access-list 135 permit ip host 10.10.129.2 any

access-list 135 permit ip any host 10.10.129.2

access-list 135 permit ip host 10.10.129.3 any

access-list 135 permit ip any host 10.10.129.3

access-list 135 permit ip host 10.10.129.4 any

access-list 135 permit ip any host 10.10.129.4

access-list 135 permit ip 10.10.129.0 0.0.0.15 any

access-list 135 permit ip any 10.10.129.0 0.0.0.15

snmp-server community tppsa RO

snmp-server community tppsaw RW (No se configurará por seguridad)

route-map TecoNet permit 10

match ip address 30

set ip next-hop 10.11.128.1 (en principio en deshuso)

!

!

control-plane (Protocolo de Cisco asociado a cef)

!

banner login ^C-----------------------------------------------------------------------

These is a device property of TPP SA

All unauthorized use will be traced and prosecuted

For more information contact - TPP SA +54 11 43723310 - www.tpp.com.ar

-----------------------------------------------------------------------^C (Se configura en Vyatta)

!

line con 0 (Se configura en Vyatta)

login local

line aux 0

line vty 0 4

privilege level 15

login local

transport input telnet

line vty 5 15

privilege level 15

login local

transport input telnet

!

scheduler allocate 20000 1000 (Garantiza CPU)

ntp clock-period 17179999

ntp update-calendar

ntp server 192.43.244.18 prefer (IP no válida, se configure otra en Vyatta)

!

end