Group Five

Network Documentation

[Device Accounts/Passwords 2](#_318srvtrcv2c)

[IP Addressing 4](#_wrukyecizym0)

[Logical Topology 6](#_9s5lf449dk2l)

[Physical Topology 7](#_ooczyiqm8112)

[New York Rack 8](#_guzv6ct6yfw5)

[Texas Rack 9](#_migxkav595pn)

[California Rack 10](#_faoxjj66dcef)

[Virtual Rack 11](#_biz893u2whm6)

[Device Inventory 12](#_7ucaq8hstq5x)

[Network Security Policy 14](#_x57v05d5ilo6)

[User Policy 16](#_cyefimnniovy)

[Exigency Planning 17](#_l85h8t3tbty2)

[Device Configurations 18](#_5d6k3rmnntfa)

[ISP Config 18](#_al1cldt3e9dg)

[HQ Config 29](#_eji61i3q0ox7)

[Branch-2 Config 41](#_semq1pkw1dei)

[Branch-3 Config 53](#_prgn28pueyhn)

[Linux Server Config 63](#_j2ul1hmiygsg)

*Members: Christopher O’Keefe, Ray Teafatiller, Allandra Waldera*

*Capstone297 - Spring 2023*

# Device Accounts/Passwords

| **Device/Accounts** | **Username** | **Password** |
| --- | --- | --- |
| PC1, PC2, PC3 | Capstone | Capstone |
| WindowServer1 | Administrator | Capstone$ |
| WindowServer2 | Administrator | Capstone05 |
| Active Directory | capstone\allandra | Capstone$ |
| Active Directory | capstone\christopher | Capstone$ |
| Active Directory | capstone\ray | Capstone$ |
| Linux Server | Root User | password |
| ISP, R1, R2, R3 | enable=password | password=password |
| ISP SSH | newyork | password |
| R1 SSH | newyork | password |
| R2 SSH | texas | password |
| R3 SSH | cal | password |

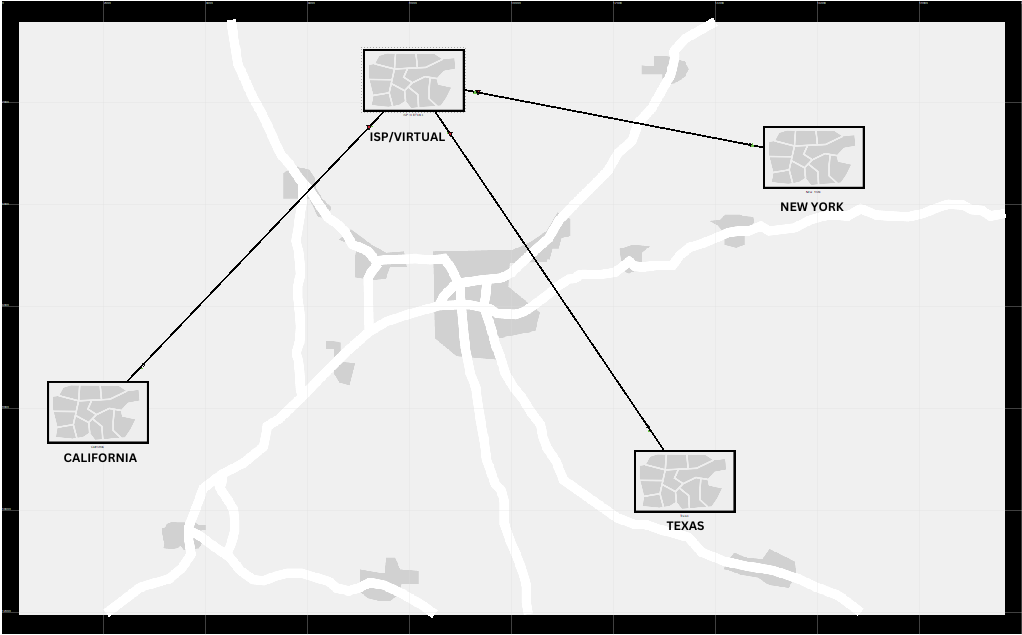
# IP Addressing

| **Devices** | **Interface** | **Device Types (Router, Host)** | **IPv4 Address** | **Subnet Mask** | **Default Gateway** | **IPv6 Address** |
| --- | --- | --- | --- | --- | --- | --- |
| PC1 | NIC | Host | 10.82.44.66 | 255.255.255.192 | 10.82.44.65 | fe80::1dd2:2893:ab4e:3bc5 |
| PC2 | NIC | Host | 10.82.44.130 | 255.255.255.224 | 10.82.44.129 | fe80::fe4a:a74d:a519:e7b9 |
| PC3 | NIC | Host | 10.82.44.161 | 255.255.255.224 | 10.82.44.162 | fe80::7c9a:2862:332d:1783 |
| ISP | G1 | Router | 10.82.44.25 | 255.255.255.192 | 10.82.44.1 |  |
| ISP | G2 | Router | 10.82.44.193 | 255.255.255.248 |  | FD03::1:1/124  FE80:: link-local |
| ISP | G3 | Router | 10.82.44.201 | 255.255.255.248 |  | FD03::2:1/124  FE80:: link-local |
| ISP | G4 | Router | 10.82.44.209 | 255.255.255.248 |  | FD03::3:1/124  FE80:: link-local |
| HQ | G1 | Router | 10.82.44.194 | 255.255.255.248 |  | FD03::1:1/124 autoconfig |
| HQ | G2 | Router | 10.82.44.218 | 255.255.255.248 |  | FD03::1:11/124 autoconfig |
| HQ | G3 | Router | 10.82.44.65 | 255.255.255.224 |  | FD03::1:20/124 |
| Branch-2 | G1 | Router | 10.82.44.210 | 255.255.255.248 |  | FD03::3:2/124 autoconfig |
| Branch-2 | G2 | Router | 10.82.44.217 | 255.255.255.248 |  | FD03::3:22/124 autoconfig |
| Branch-2 | G3 | Router | 10.82.44.129 | 255.255.255.248 |  | FD03::3:32/124 autoconfig |
| Branch-2 | G4 | Router | 10.82.44.225 | 255.255.255.248 |  | FD03::3:42/124 autoconfig |
| Branch-3 | G1 | Router | 10.82.44.202 | 255.255.255.248 |  | FD03::2:2/124 autoconfig |
| Branch-3 | G2 | Router | 10.82.44.226 | 255.255.255.248 |  | FD03::2:10/124 autoconfig |
| Branch-3 | G3 | Router | 10.82.44.161 | 255.255.255.248 |  | FD03::3:22/124 autoconfig |
| Linux Server | R1 | Host | 10.82.44.90 | 255.255.255.192 | 10.82.44.65 | fe80::20c:29ff:feb9:806d |
| Windows Server1 | R3 | Host | 10.82.44.164 | 255.255.255.224 | 10.82.44.1 | fe80::8d31:3772:a31:4ffb |
| Windows Server2 | R2 | Host | 10.82.44.144 | 255.255.255.224 | 10.82.44.1 | fdd1:2a92:b5dd:333::1 |

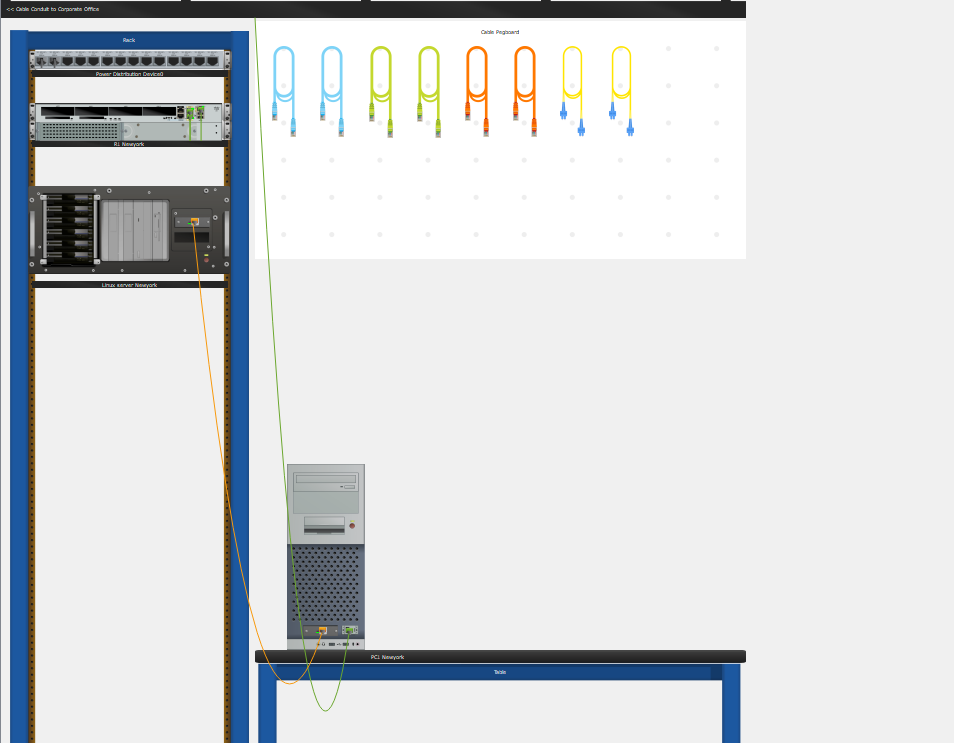
# Logical Topology

# 

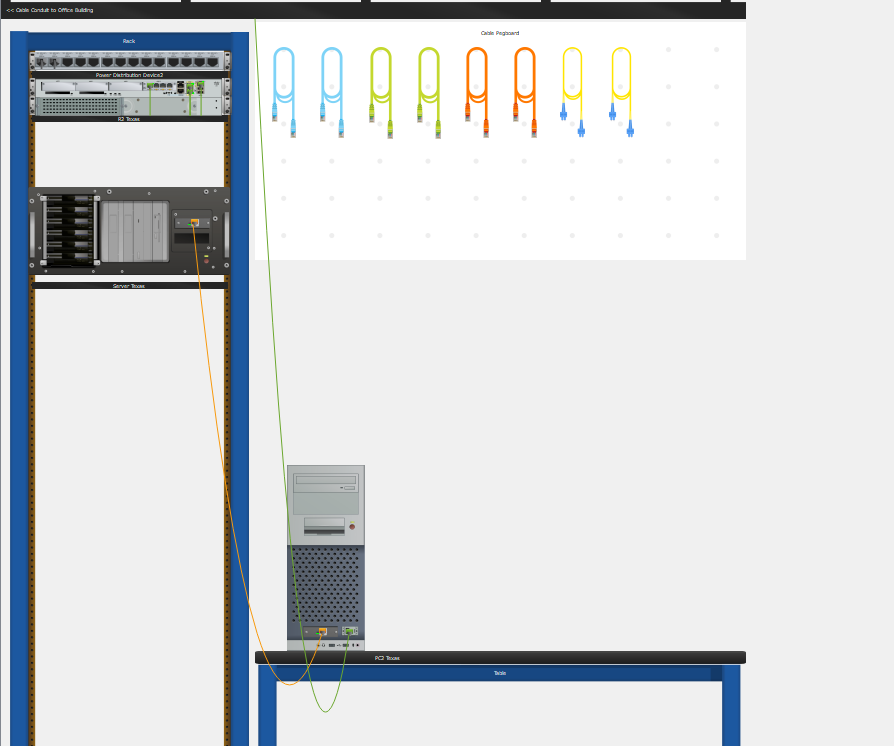
# Physical Topology

****

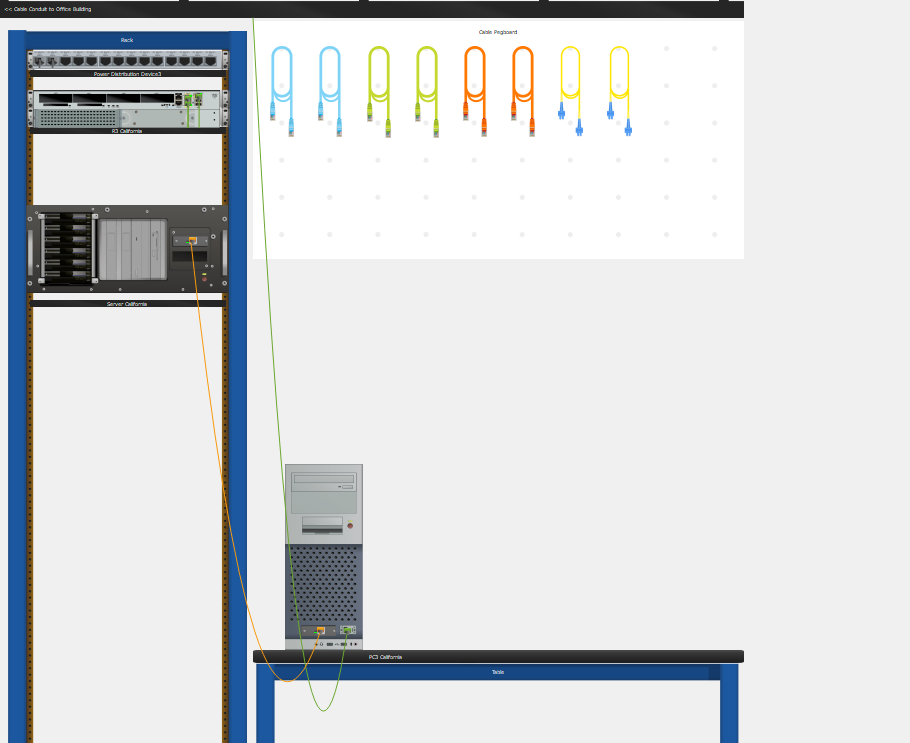
# New York Rack

****

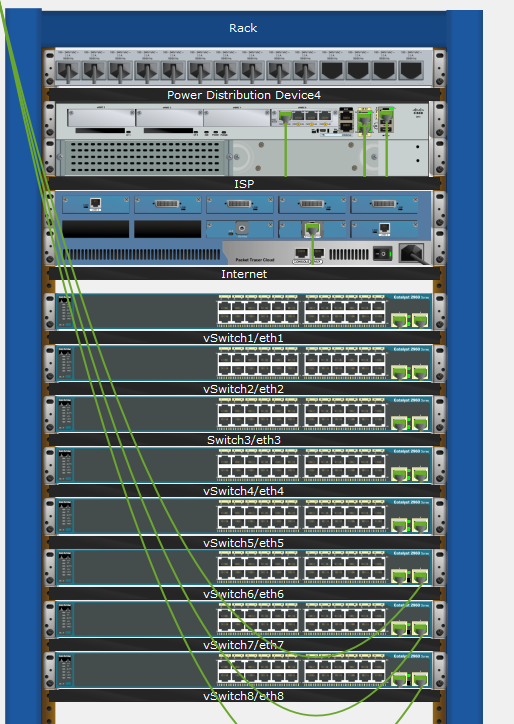
# Texas Rack

****

# California Rack

****

# Virtual Rack

****

# Device Inventory

* Cisco 2911 Router, hostname: HQ

NAME: "Chassis", DESCR: "Cisco CSR1000V Chassis"

PID: CSR1000V , VID: V00 , SN: 9KDE15AICAQ

NAME: "module R0", DESCR: "Cisco CSR1000V Route Processor"

PID: CSR1000V , VID: V00 , SN: JAB1303001C

NAME: "module F0", DESCR: "Cisco CSR1000V Embedded Services Processor"

PID: CSR1000V , VID: , SN:

* Cisco 2911 Router, hostname: Branch2,

NAME: "Chassis", DESCR: "Cisco CSR1000V Chassis"

PID: CSR1000V , VID: V00 , SN: 9J8PBBF3X02

NAME: "module R0", DESCR: "Cisco CSR1000V Route Processor"

PID: CSR1000V , VID: V00 , SN: JAB1303001C

NAME: "module F0", DESCR: "Cisco CSR1000V Embedded Services Processor"

PID: CSR1000V , VID: , SN:

* Cisco 2911 Router, hostname: Branch3

NAME: "Chassis", DESCR: "Cisco CSR1000V Chassis"

PID: CSR1000V , VID: V00 , SN: 9J2TH7JSMUV

NAME: "module R0", DESCR: "Cisco CSR1000V Route Processor"

PID: CSR1000V , VID: V00 , SN: JAB1303001C

NAME: "module F0", DESCR: "Cisco CSR1000V Embedded Services Processor"

PID: CSR1000V , VID: , SN:

* Virtual Cisco Switch
* Virtual Cisco Switch
* Virtual Cisco Switch
* Virtual Cisco Switch
* Virtual Cisco Switch
* Virtual Cisco Switch
* Virtual Cisco Switch
* Virtual Cisco Switch
* Windows 10 (64-bit) PC, hostname: PC1NewYork.capstone.local,

Serial: VMWare-56 4d 6c 3b dc f7 d2 61-78 03 36 85 c0 85 b6 0b

* Windows 10 (64-bit) PC, hostname: Texas.capstone.local,

Serial: VMWare-56 4d 8a 3b 03 f7 50 b3-7d a9 0d ba ef f2 94 d9

* Windows 10 (64-bit) PC, hostname: PC3California.capstone.local,

Serial: VMWare-56 4d b8 c0 6a b3 c1 99-d1 af 88 d9 46 ed 9e 64

* Microsoft Windows Server 2016, hostname: WindowsServer1.capstone.local,

Serial: VMWare-56 4d a0 df a8 b7 f8 70-47 b7 24 62 8f b8 6d 94

* Microsoft Windows Server 2016, hostname: WindowsServer2.capstone.local,

Serial: VMWare-56 4d 94 27 8d 13 c9 43-06 0d df 74 33 45 d3 0c

* RHEL 8 Server, hostname: linux.capstone.local,

Serial: VMWare-56 4d 8e 8c 02 67 a4 67-e2 97 a5 45 a2 b9 80 6d

# 

# Network Security Policy

1. Introduction

* Purpose and scope of the security policy
* Overview of the organization's commitment to security

1. Security Objectives

* Protection of sensitive data and information
* Prevention of unauthorized access and data breaches
* Compliance with relevant laws and regulations

1. Roles and Responsibilities

* Designation of security roles and responsibilities
* Accountability for security incidents and breaches

1. Access Control

* User authentication and authorization procedures
* Password complexity and expiration policies
* Use of multi-factor authentication where applicable

1. Network Security

* Firewall configuration and management
* Intrusion detection and prevention systems (IDPS)
* Regular security audits and vulnerability assessments

1. Data Protection

* Encryption of sensitive data in transit and at rest
* Data backup and recovery procedures
* Data classification and handling guidelines

1. Incident Response

* Reporting and escalation procedures for security incidents
* Investigation and mitigation of security breaches
* Lessons learned and continuous improvement processes

1. Employee Awareness and Training

* Security awareness programs for all employees
* Regular training on security best practices and policies

1. Compliance and Legal Requirements

* Adherence to applicable laws, regulations, and industry standards
* Protection of customer privacy and data

1. Policy Review and Updates

* Regular review and update of the security policy
* Communication of policy changes to employees

# User Policy

1. Acceptable Use

* Guidelines for appropriate use of organizational resources
* Prohibition of unauthorized access or use of systems

1. Password Security

* Password complexity requirements
* Prohibition of sharing passwords or using default passwords

1. Access Control

* Authorization procedures for accessing specific resources
* Restrictions on sharing or transferring access credentials

1. Data Handling

* Guidelines for protecting sensitive data
* Classification of data and appropriate handling measures

1. Internet and Email Usage

* Acceptable web browsing and email practices
* Prohibition of downloading or sharing unauthorized content

1. Remote Access

* Secure connection requirements for remote access
* Prohibition of unauthorized remote access tools

1. Incident Reporting

* Procedures for reporting security incidents or suspected breaches
* Protection of whistleblowers and non-retaliation policy

1. Personal Device Usage

* Guidelines for using personal devices on the organizational network
* Compliance with security requirements for personal devices

1. Consequences of Non-Compliance

* Disciplinary actions for policy violations
* Suspension or termination of user privileges in severe cases

# Exigency Planning

1. Introduction

* Purpose and scope of the exigency planning document
* Overview of potential network emergencies and disruptions

1. Risk Assessment

* Identification of potential risks and threats to the network
* Assessment of their impact and likelihood

1. Exigency Measures

* Redundancy and fault tolerance measures
* Backup power supply (UPS) for critical network components
* Redundant network links and alternative communication channels

1. Disaster Recovery Plan

* Backup and recovery procedures for critical data and systems
* Off-site data storage and regular backups
* Testing and validation of the disaster recovery plan

1. Business Continuity Plan

* Procedures for maintaining essential business operations during emergencies
* Allocation of resources and responsibilities
* Communication and coordination protocols

1. Emergency Communication

* Contact information for key personnel and stakeholders
* Communication channels during emergencies
* Escalation procedures and reporting lines

1. Testing and Training

* Regular testing of exigency plans and procedures
* Training sessions for employees on emergency response protocols

1. Post-Incident Analysis and Improvement

* Analysis of emergency incidents and lessons learned
* Continuous improvement of exigency plans and measures

# Device Configurations

## ISP Config

version 16.12

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

service call-home

platform qfp utilization monitor load 80

platform punt-keepalive disable-kernel-core

platform console auto

!

hostname ISP

!

boot-start-marker

boot-end-marker

!

!

vrf definition california

!

address-family ipv4

exit-address-family

!

address-family ipv6

exit-address-family

!

vrf definition newyork

ipv6 multicast multitopology

!

address-family ipv4

exit-address-family

!

address-family ipv6

exit-address-family

!

vrf definition texas

!

enable secret 9 $9$NTDNEhDlEix/3U$gVDGRPJ3DSwCnPU37C22BphpTRaE1pvuMWXTzcVY.VE

enable password 7 060503205F5D

!

aaa new-model

aaa local authentication default authorization default

!

aaa session-id common

call-home

! If contact email address in call-home is configured as sch-smart-licensing@cisco.com

! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH notifications.

contact-email-addr sch-smart-licensing@cisco.com

profile "CiscoTAC-1"

active

destination transport-method http

no destination transport-method email

!

ip name-server 10.82.44.166 10.82.44.144 10.82.44.90 8.8.8.8

ip domain name capstone.local

!

login on-success log

ipv6 unicast-routing

ipv6 dhcp pool IPV6\_DHCPPOOL

!

ipv6 rip vrf-mode enable

ipv6 multicast-routing

!

subscriber templating

!

multilink bundle-name authenticated

!

voice service voip

allow-connections sip to sip

supplementary-service media-renegotiate

sip

registrar server expires max 120 min 60

!

voice register global

mode cme

source-address 10.82.44.25 port 5060

max-dn 1200

max-pool 475

auto-register

!

crypto pki trustpoint TP-self-signed-775802846

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-775802846

revocation-check none

rsakeypair TP-self-signed-775802846

!

crypto pki trustpoint SLA-TrustPoint

enrollment pkcs12

revocation-check crl

!

!

crypto pki certificate chain TP-self-signed-775802846

crypto pki certificate chain SLA-TrustPoint

!

crypto pki certificate pool

cabundle nvram:ios\_core.p7b

!

license udi pid CSR1000V sn 9VKLYRR7D3X

diagnostic bootup level minimal

memory free low-watermark processor 72314

!

!

et-analytics

!

spanning-tree extend system-id

!

username isp privilege 14 secret 9 $9$3VUH2/6D2V.J3E$GZ0KcPzb5xJj74Tn1ly62PZoEwJ2DLkHNkEZs53UmWI

username ray privilege 15 secret 9 $9$2lQG2/EI4/AG3.$i2tOx..bhPMAc6kqi3bq.eghR39Vn3wj7W4wpdOxcCU

user-name admin

creation-time 1684877615

password 7 105E080A16001D1908

!

redundancy

!

!

!

crypto ikev2 client flexvpn ray

!

!

class-map type inspect match-any INSIDE\_DMZ\_PROTOCOLS

match access-group name INSIDE\_DMZ

class-map type inspect match-any INSIDE\_OUTSIDE\_PROTOCOLS

match protocol http

match protocol https

match protocol dns

match protocol tcp

match protocol udp

match protocol icmp

match protocol pop3

match protocol smtp

match protocol ftp

match protocol sip

match protocol tftp

match protocol rtsp

match protocol imap

match protocol pptp

match protocol telnet

match protocol ssh

match protocol ipsec-msft

class-map type inspect match-any OUTSIDE\_INSIDE\_PROTOCOLS

match access-group name OUTSIDE\_INSIDE

class-map type inspect match-any OUTSIDE\_DMZ\_PROTOCOLS

match access-group name OUTSIDE\_DMZ

!

policy-map type inspect INSIDE\_OUTSIDE\_POLICY

class type inspect INSIDE\_OUTSIDE\_PROTOCOLS

inspect

class class-default

policy-map type inspect OUTSIDE\_DMZ\_POLICY

class type inspect OUTSIDE\_DMZ\_PROTOCOLS

inspect

class class-default

policy-map type inspect INSIDE\_DMZ\_POLICY

class type inspect INSIDE\_DMZ\_PROTOCOLS

pass

class class-default

policy-map type inspect OUTSIDE\_INSIDE\_POLICY

class type inspect OUTSIDE\_INSIDE\_PROTOCOLS

pass

class class-default

!

zone security DMZ

description restricted network

zone security INSIDE

description capstone.local

zone security OUTSIDE

description global network

zone-pair security INSIDE\_DMZ source INSIDE destination DMZ

service-policy type inspect INSIDE\_DMZ\_POLICY

zone-pair security INSIDE\_OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect INSIDE\_OUTSIDE\_POLICY

zone-pair security OUTSIDE\_DMZ source OUTSIDE destination DMZ

service-policy type inspect OUTSIDE\_DMZ\_POLICY

zone-pair security OUTSIDE\_INSIDE source OUTSIDE destination INSIDE

service-policy type inspect OUTSIDE\_INSIDE\_POLICY

!

!

crypto isakmp policy 8

encryption aes 256

hash sha512

authentication pre-share

group 24

!

crypto isakmp policy 9

encryption aes 256

hash sha512

authentication pre-share

group 24

crypto isakmp key Capstone$ address 0.0.0.0

!

!

crypto ipsec transform-set MY\_SET esp-aes 256 esp-sha512-hmac

mode tunnel

!

!

!

crypto map MY\_MAP 1 ipsec-isakmp

! Incomplete

match address 100

crypto map MY\_MAP 10 ipsec-isakmp

set peer 10.82.44.194

set transform-set MY\_SET

match address 100

crypto map MY\_MAP 20 ipsec-isakmp

! Incomplete

set peer 10.82.44.210

set transform-set MY\_SET

crypto map MY\_MAP 30 ipsec-isakmp

set peer 10.82.44.202

set transform-set MY\_SET

match address 100

!

!

interface Loopback0

ip dhcp relay information trusted

ip address 10.0.0.1 255.255.255.255

ipv6 address dhcp rapid-commit

ipv6 address FE80:: link-local

ipv6 address 2001:DB8::E000:0:0:F/64

ipv6 address FD01:ABAB::/64 eui-64

ipv6 address autoconfig

!

interface Tunnel10

no ip address

!

interface Tunnel30

no ip address

!

interface Tunnel40

no ip address

!

interface Tunnel50

no ip address

!

interface GigabitEthernet1

description internet www

ip address 10.82.44.25 255.255.255.192

ip nat outside

negotiation auto

no mop enabled

no mop sysid

!

interface GigabitEthernet2

description ISP to R1

ip address 10.82.44.193 255.255.255.248

ip nat inside

ip ospf 1 area 0

negotiation auto

ipv6 address FE80:: link-local

ipv6 address FD03::1:1/124

ipv6 address autoconfig

no mop enabled

no mop sysid

crypto map MY\_MAP

!

interface GigabitEthernet2.10

!

interface GigabitEthernet3

description ISP to R3

ip address 10.82.44.201 255.255.255.248

ip nat inside

ip ospf 1 area 0

negotiation auto

ipv6 address FE80:: link-local

ipv6 address FD03::2:1/124

ipv6 address autoconfig

ipv6 enable

ipv6 ospf 1 area 0

no mop enabled

no mop sysid

crypto map MY\_MAP

!

interface GigabitEthernet3.20

!

interface GigabitEthernet3.30

!

interface GigabitEthernet4

description ISP to R2

ip address 10.82.44.209 255.255.255.248

ip nat inside

ip ospf 1 area 0

negotiation auto

ipv6 address FE80:: link-local

ipv6 address FD03::3:1/124

ipv6 address autoconfig default

ipv6 enable

ipv6 ospf 1 area 0

no mop enabled

no mop sysid

crypto map MY\_MAP

!

router ospf 1

router-id 10.82.44.1

network 10.82.44.0 0.0.0.63 area 0

network 10.82.44.192 0.0.0.7 area 0

network 10.82.44.200 0.0.0.7 area 0

network 10.82.44.208 0.0.0.7 area 0

network 10.82.44.0 0.0.0.255 area 0

!

ip default-gateway 10.82.44.1

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

!

ip nat pool NAT 192.0.2.1 192.0.2.253 netmask 255.255.255.0

ip nat inside source list NAT pool NAT overload

ip dns server

ip route 0.0.0.0 0.0.0.0 10.82.44.1

ip route 192.0.2.0 255.255.255.192 GigabitEthernet2

ip route 192.0.2.64 255.255.255.192 GigabitEthernet3

ip route 192.0.2.128 255.255.255.224 GigabitEthernet3

ip route vrf newyork 0.0.0.0 0.0.0.0 192.168.12.1

ip route vrf california 0.0.0.0 0.0.0.0 192.168.23.3

ip ssh version 2

!

ip access-list standard NAT

!

ip access-list extended INSIDE\_DMZ

10 permit tcp any 10.82.44.0 0.0.0.255 eq www

20 permit icmp any 10.82.44.0 0.0.0.255

ip access-list extended OUTSIDE\_DMZ

10 permit tcp any 10.82.44.0 0.0.0.255 eq www

ip access-list extended OUTSIDE\_INSIDE

10 permit icmp any 10.82.44.0 0.0.0.255

!

ip access-list standard 1

10 permit 10.82.44.0 0.0.0.63

ip access-list extended 100

10 permit ip host 10.82.44.25 host 10.82.44.65

20 permit ip host 10.82.44.25 host 10.82.44.129

30 permit ip host 10.82.44.25 host 10.82.44.161

ipv6 router ospf 1

!

!

!

!

!

!

!

!

control-plane

!

!

!

!

telephony-service

max-dn 1200

ip source-address 10.82.44.25 port 2000

max-conferences 8 gain -6

transfer-system full-consult

!

!

!

banner motd ^C Authorized Access Only!

Next time i'll Distributes Denial-of-Service ^C

!

line con 0

password 7 071F205F5D1E161713

stopbits 1

line vty 0 4

password 7 071F205F5D1E161713

transport input ssh

!

!

end

## HQ Config

platform console virtual

!

hostname HQ

enable secret 9 $9$L8Tzwi8puZxIr.$ubirlZZLNlD3vd5M7E0WHGW5ljzzkDlv0KVfSsnki4Y

12

rd 12:12

route-target export 12:12

route-target import 23:23

!

ip vrf 23

ip host capstone.local 10.100.0.251

ip host linux.capstone.local 10.82.44.90

ip host PC1NewYork.capstone.local 10.82.44.66

ip host PC2Texas.capstone.local 10.82.44.130

ip host PC3California.capstone.local 10.82.44.162

ip host windowserver1.capstone.local 10.82.44.164

ip host windowserver2.capstone.local 10.82.44.144

ip host windowserver1.capstone.local-rtp 10.82.44.164

ip host windowserver2.capstone.local-rtp 10.82.44.144

ip name-server 10.82.44.90 10.82.44.66

ip domain list capstone.local

ip domain list linux.capstone.local

ip domain name capstone.local

crypto pki trustpoint TP-self-signed-4048043088

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-4048043088

revocation-check none

rsakeypair TP-self-signed-4048043088

!

crypto pki trustpoint SLA-TrustPoint

enrollment pkcs12

revocation-check crl

!

!

crypto pki certificate chain TP-self-signed-4048043088

crypto pki certificate chain SLA-TrustPoint

!

crypto pki certificate pool

cabundle nvram:ios\_core.p7b

!

license udi pid CSR1000V sn 9KDE15AICAQ

diagnostic bootup level minimal

memory free low-watermark processor 72314

!

!

et-analytics

!

spanning-tree extend system-id

!

username newyork secret 9 $9$4393NApvhEghcU$HevY4n0MOENs/ORcTA7RyI5AYWOV98Zkqggd7lx5jG6

username webui privilege 14 password 7 105E080A16001D1908

username ray privilege 15 secret 9 $9$2FQF2lUD3V2H2.$or.XTHP/ovniwTIE2pqzfrIQo0YAx4G8uwsqcFKCRvM

!

redundancy

!

crypto ikev2 proposal WEBUI-PROPOSAL-Tunnel2

encryption aes-cbc-256 aes-cbc-192 aes-cbc-128

integrity sha512 sha384 sha256 sha1 md5

group 2 5

crypto ikev2 proposal WEBUI-PROPOSAL-Tunnel3

encryption aes-cbc-256 aes-cbc-192 aes-cbc-128

integrity sha512 sha384 sha256 sha1 md5

group 2 5

!

crypto ikev2 policy WEBUI-POLICY

match fvrf any

proposal WEBUI-PROPOSAL-Tunnel2

proposal WEBUI-PROPOSAL-Tunnel3

!

crypto ikev2 keyring WEBUI-KEYS

peer WEBUI-PEER-10.82.44.160

description KEY-PEER-10.82.44.160

address 10.82.44.160 255.255.255.0

pre-shared-key Capstone$

!

peer WEBUI-PEER-10.82.44.130

description KEY-PEER-10.82.44.130

pre-shared-key Capstone$

!

!

!

crypto ikev2 profile WEBUI-IKEV2-PROFILE

match fvrf any

match identity remote address 10.82.44.160 255.255.255.255

match identity remote address 10.82.44.130 255.255.255.255

authentication remote pre-share

authentication local pre-share

keyring local WEBUI-KEYS

!

!

class-map type inspect match-any Web\_app

match protocol tcp

match protocol udp

match protocol ftp

match protocol icmp

class-map type inspect match-all Web

match class-map Web\_app

match access-group name Web\_acl

!

policy-map type inspect INSIDE-OUTSIDE-POLICY

class type inspect Web

inspect

class class-default

drop log

!

zone security INSIDE

description Zone for inside interfaces

zone security OUTSIDE

description Zone for outside interfaces

zone security default

zone-pair security INSIDE-OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect INSIDE-OUTSIDE-POLICY

crypto ipsec transform-set WEBUI-TS-Tunnel2 esp-aes esp-sha256-hmac

mode tunnel

crypto ipsec transform-set WEBUI-TS-Tunnel3 esp-aes esp-sha-hmac

mode tunnel

!

crypto ipsec profile WEBUI-IPSEC-PROFILE-Tunnel2

set transform-set WEBUI-TS-Tunnel2

set ikev2-profile WEBUI-IKEV2-PROFILE

!

crypto ipsec profile WEBUI-IPSEC-PROFILE-Tunnel3

set transform-set WEBUI-TS-Tunnel3

set ikev2-profile WEBUI-IKEV2-PROFILE

!

!

!

crypto map MY\_MAP 1 ipsec-isakmp

set peer 10.82.44.193

set transform-set MY\_SET

match address 100

crypto map MY\_MAP 9 ipsec-isakmp

crypto map MY\_MAP 30 ipsec-isakmp

set peer 10.82.44.201

description router id

interface Loopback0

description router id

ip dhcp relay information trusted

ip address 1.1.1.1 255.255.255.255

!

interface Loopback1

description loop back for eigrp advertimsment

ip vrf forwarding 12

ip dhcp relay information trusted

ip address 1.1.1.1 255.255.255.0

!

interface Port-channel12

description ip vrf forwarding 12

ip vrf forwarding 12

ip dhcp relay information trusted

ip address 192.168.112.1 255.255.255.0 secondary

ip address 192.168.12.1 255.255.255.0

no negotiation auto

no mop enabled

no mop sysid

spanning-tree portfast

!

interface Tunnel1

description IPv6 over IPv4 GRE Tunnel Protection

no ip address

ipv6 address ::7271:0:0:0:11/64

ipv6 address 0:0:0:7271::/64 eui-64

tunnel source GigabitEthernet1

tunnel destination 10.82.44.25

!

interface Tunnel2

description VPN r1 to r3 win1

no ip address

tunnel source GigabitEthernet1

tunnel mode ipsec ipv4

tunnel destination 10.82.44.160

tunnel protection ipsec profile WEBUI-IPSEC-PROFILE-Tunnel2

!

interface Tunnel3

description pc1 to pc2

no ip address

tunnel source GigabitEthernet2

tunnel mode ipsec ipv4

tunnel destination 10.82.44.130

tunnel protection ipsec profile WEBUI-IPSEC-PROFILE-Tunnel3

!

interface Tunnel10

description IPv6 over IPv4 GRE Tunnel Protection

no ip address

ipv6 address ::7272:0:0:0:72/64

tunnel source GigabitEthernet1

tunnel destination 10.82.44.193

!

interface Tunnel30

no ip address

no ip redirects

tunnel mode ipv6ip 6to4

!

interface GigabitEthernet1

description R1 to ISP

ip address 10.82.44.194 255.255.255.248

ip nat inside

ip ospf 1 area 0

negotiation auto

ipv6 address FD03::1:1/124

ipv6 address autoconfig

ipv6 enable

ipv6 ospf 1 area 0

no mop enabled

no mop sysid

crypto map MY\_MAP

!

interface GigabitEthernet2

description r1 to r2

ip address 10.82.44.217 255.255.255.248

ip nat inside

ip ospf 1 area 0

negotiation auto

ipv6 address FD03::1:11/124

ipv6 address autoconfig

no mop enabled

no mop sysid

crypto map MY\_MAP

!

interface GigabitEthernet3

description "Connection to R2"

ip address 10.82.44.65 255.255.255.192

ip nat inside

ip ospf 1 area 0

negotiation auto

ipv6 address FE80:: link-local

ipv6 address FD03::1:20/124

ipv6 enable

ipv6 ospf 1 area 0

no mop enabled

no mop sysid

crypto map MY\_MAP

!

router eigrp TEST

!

router eigrp virtual-name

!

address-family ipv4 unicast autonomous-system 1

!

topology base

default-metric 10000 100 255 1 1500

exit-af-topology

network 10.82.44.0 0.0.0.255

exit-address-family

!

router eigrp 12

network 0.0.0.0

!

router eigrp 23

network 0.0.0.0

!

router lisp

exit

!

router ospf 1

router-id 1.1.1.1

network 10.82.44.64 0.0.0.63 area 0

network 10.82.44.192 0.0.0.7 area 0

network 10.82.44.216 0.0.0.7 area 0

network 10.82.44.0 0.0.0.255 area 0

network 10.82.0.0 0.0.255.255 area 0

!

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

!

ip nat pool capstone 192.0.2.1 192.0.2.62 netmask 255.255.255.192

ip nat inside source static udp 10.82.44.194 5353 interface GigabitEthernet1 5353

ip nat inside source list 1 pool capstone

ip nat inside source list NAT-ACL interface GigabitEthernet1 overload

ip route 0.0.0.0 0.0.0.0 10.82.44.193

ip route 10.82.44.64 255.255.255.192 Tunnel3

ip route 10.82.44.128 255.255.255.224 Tunnel3

ip route 10.82.44.160 255.255.255.224 Tunnel2

ip route 10.82.44.160 255.255.255.224 Tunnel3

ip route 192.0.2.0 255.255.255.192 GigabitEthernet1

ip ssh version 2

!

ip access-list extended ABC

10 permit ip any any

ip access-list extended NAT-ACL

10 deny ip any 10.82.44.160 0.0.0.31

ip access-list extended Web\_acl

10 permit ip any any

!

ip access-list standard 1

10 permit 10.82.44.0 0.0.0.63

ip access-list extended 100

10 permit ip host 10.82.44.65 host 10.82.44.129

20 permit ip host 10.82.44.65 host 10.82.44.161

30 permit ip host 10.82.44.65 host 10.82.44.25

ip access-list extended 101

10 permit udp any any eq domain

20 permit udp any eq domain any

ipv6 router ospf 1

!

control-plane

!

banner motd ^CAuthorize Users Only!^C

!

line con 0

password 7 12090404011C03162E

stopbits 1

line vty 0 4

password 7 140713181F13253920

length 0

transport input ssh

!

!

end

## Branch-2 Config

platform console virtual

!

hostname texas

!

boot-start-marker

boot-end-marker

!

enable secret 9 $9$ZmHcdS3MnQU95E$bTf.S1dMD.ONoesjOXkJXid5OW5DwZeQO8s9s2H2JcE

enable password 7 044B0A151C36435C0D

ip vrf 12

rd 12:12

route-target export 12:12

route-target import 23:23

!

ip vrf 23

rd 23:23

route-target export 23:23

route-target import 12:12

!

ip nbar http-services

!

ip host capstone.local 10.100.0.251

ip host linux.capstone.local 10.82.44.90

ip host PC1NewYork.capstone.local 10.82.44.66

ip host PC2Texas.capstone.local 10.82.44.130

ip host PC3California.capstone.local 10.82.44.162

ip host windowserver1.capstone.local 10.82.44.164

ip host windowserver2.capstone.local 10.82.44.144

ip host windowserver1.capstone.local-rtp 10.82.44.164

ip host windowserver2.capstone.local-rtp 10.82.44.144

ip name-server 10.82.44.144 10.82.44.130

ip domain name capstone.local

!

ip dhcp pool 1

utilization mark high 80 log

utilization mark low 70 log

network 172.16.0.0 255.255.0.0

bootfile xllboot

next-server 172.17.1.103 172.17.2.103

domain-name capstone.local

dns-server 10.82.44.164 10.100.0.251

netbios-name-server 172.16.1.103 172.16.2.103

netbios-node-type h-node

default-router 172.16.1.100 172.16.1.101

option 19 hex 01

lease 30

!

!

login on-success log

ipv6 unicast-routing

ipv6 dhcp pool IPV6\_DHCPPOOL

address prefix 2001:DB8:5:10::/64

key chain to-r3

key 23

key-string 7 08316C5D1A0E550516

crypto pki trustpoint TP-self-signed-2576812301

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-2576812301

revocation-check none

rsakeypair TP-self-signed-2576812301

!

crypto pki trustpoint SLA-TrustPoint

enrollment pkcs12

revocation-check crl

!

!

crypto pki certificate chain TP-self-signed-2576812301

crypto pki certificate chain SLA-TrustPoint

!

license udi pid CSR1000V sn 9J8PBBF3X02

diagnostic bootup level minimal

memory free low-watermark processor 72314

!

!

et-analytics

!

spanning-tree extend system-id

!

username admin password 7 044B0A151C36435C0D

username texas password 7 105E080A16001D1908

user-name ray

creation-time 1685709868

privilege 15

password 7 111918160405041E00

!

redundancy

!

!

cdp run

!

!

class-map type inspect match-any Web\_app

match protocol tcp

match protocol udp

match protocol ftp

match protocol icmp

class-map type inspect match-all Web

match class-map Web\_app

match access-group name Web\_acl

!

policy-map type inspect INSIDE-OUTSIDE-POLICY

class type inspect Web

inspect

class class-default

drop log

!

zone security INSIDE

description Zone for inside interfaces

zone security OUTSIDE

description Zone for outside interfaces

zone security default

zone-pair security INSIDE-OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect INSIDE-OUTSIDE-POLICY

crypto map MY\_MAP 1 ipsec-isakmp

set peer 10.82.44.209

set transform-set MY\_SET

match address 100

crypto map MY\_MAP 9 ipsec-isakmp

! Incomplete

set transform-set MY\_SET

!

interface Loopback0

description r id

ip dhcp relay information trusted

ip address 2.2.2.2 255.255.255.0

ipv6 address 2001:DB8::E000:0:0:F/64 anycast

ipv6 address FD04:ABAB::/64 eui-64

interface Loopback12

ip dhcp relay information trusted

ip address 12.12.12.12 255.255.255.255

!

interface Loopback23

description "Loopback for EIGRP advertisement"

ip vrf forwarding 23

ip dhcp relay information trusted

ip address 23.23.23.23 255.255.255.255

!

interface Port-channel12

description Connection to R1

ip vrf forwarding 12

ip address 192.168.112.2 255.255.255.0 secondary

ip address 192.168.12.2 255.255.255.0

no negotiation auto

ipv6 address dhcp rapid-commit

ipv6 address FD03::2:112/124

ipv6 address FD03::2:222/124

ipv6 address FD03::2:332/124

no mop enabled

no mop sysid

spanning-tree portfast trunk

!

interface Port-channel23

description Connection to R2

ip vrf forwarding 23

ip address 192.168.123.2 255.255.255.0 secondary

ip address 192.168.23.2 255.255.255.0

no negotiation auto

ipv6 address dhcp rapid-commit

ipv6 address FD03::12:2/124

ipv6 address FD03::22:2/124

ipv6 address FD03::32:2/124

ipv6 address autoconfig

no mop enabled

no mop sysid

spanning-tree portfast trunk

!

interface Tunnel10

description IPv6 over IPv4 GRE Tunnel Protection

no ip address

ipv6 address ::7272:0:0:0:72/64

tunnel source GigabitEthernet2

tunnel destination 10.82.44.117

!

interface Tunnel20

no ip address

!

interface Tunnel40

no ip address

!

interface GigabitEthernet1

description r2 eth3 isp

ip address 10.82.44.210 255.255.255.248

ip nat inside

ip ospf 1 area 0

negotiation auto

cdp enable

ipv6 address FD03::3:2/124

ipv6 address autoconfig

no mop enabled

no mop sysid

crypto map MY\_MAP

!

interface GigabitEthernet2

description R1 - R2

ip vrf forwarding 12

ip address 10.82.44.218 255.255.255.248

ip nat inside

negotiation auto

ipv6 address FD03::3:22/124

ipv6 address autoconfig

no mop enabled

no mop sysid

crypto map MY\_MAP

!

interface GigabitEthernet3

description r2 eth6 lan

ip address 10.82.44.129 255.255.255.224

ip nat inside

ip ospf 1 area 0

negotiation auto

ipv6 address FD03::3:32/124

ipv6 address autoconfig

no mop enabled

no mop sysid

crypto map MY\_MAP

!

interface GigabitEthernet4

description r2 to r3

ip vrf forwarding 23

ip address 10.82.44.225 255.255.255.248

ip nat inside

negotiation auto

ipv6 address FD03::3:42/124

ipv6 address autoconfig

no mop enabled

no mop sysid

!

!

router eigrp central

!

address-family ipv4 unicast vrf 12 autonomous-system 12

!

af-interface default

authentication mode md5

passive-interface

exit-af-interface

!

topology base

redistribute bgp 65535 metric 1000 100 255 1 1500

exit-af-topology

network 0.0.0.0

exit-address-family

!

address-family ipv4 unicast vrf 23 autonomous-system 23

!

af-interface GigabitEthernet4

authentication mode md5

authentication key-chain to-r3

exit-af-interface

!

af-interface Port-channel23

authentication mode md5

exit-af-interface

!

topology base

redistribute bgp 65535 metric 1000 100 255 1 1500

exit-af-topology

network 0.0.0.0

exit-address-family

!

router eigrp 12

network 0.0.0.0

!

router ospf 1

router-id 2.2.2.2

network 10.82.44.128 0.0.0.31 area 0

network 10.82.44.208 0.0.0.7 area 0

network 10.82.44.216 0.0.0.7 area 0

network 10.82.44.224 0.0.0.7 area 0

network 10.82.44.0 0.0.0.255 area 0

network 10.82.0.0 0.0.255.255 area 0

!

router bgp 65535

bgp log-neighbor-changes

!

address-family ipv4 vrf 12

redistribute eigrp 12

exit-address-family

!

address-family ipv4 vrf 23

redistribute eigrp 23

exit-address-family

!

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

!

ip nat pool capstone 192.0.2.129 192.0.2.158 netmask 255.255.255.224

ip nat inside source static udp 10.82.44.209 5354 interface GigabitEthernet1 5354

ip nat inside source list 1 pool capstone

ip route 0.0.0.0 0.0.0.0 10.82.44.209

ip route 192.0.2.64 255.255.255.192 GigabitEthernet1

ip ssh version 2

!

ip access-list extended Web\_acl

10 permit ip any any

!

ip access-list standard 1

10 permit 10.82.44.0 0.0.0.63

ip access-list extended 100

10 permit ip host 10.82.44.129 host 10.82.44.25

20 permit ip host 10.82.44.129 host 10.82.44.65

ip access-list extended 101

10 permit udp any any eq domain

20 permit udp any eq domain any

ip access-list extended 102

ipv6 router ospf 1

!

!

control-plane

!

!

banner motd ^CUnauthorized Access Is Strictly Prohibited!^C

!

line con 0

password 7 105E080A16001D1908

stopbits 1

line vty 0 4

password 7 105E080A16001D1908

length 0

transport input ssh

!

!

end

## Branch-3 Config

platform console virtual

!

hostname california

enable secret 9 $9$O58nf929w3iDoE$fzQiLvC.U6SOiLmIjj2oIp7lz1NPWkXNWH3LF/op9sE

enable password 7 13061B13181F

ip vrf 23

rd 23:23

!

!

ip nbar http-services

!

!

ip host capstone.local 10.100.0.251

ip host linux.capstone.local 10.82.44.90

ip host PC1NewYork.capstone.local 10.82.44.66

ip host PC2Texas.capstone.local 10.82.44.130

ip host PC3California.capstone.local 10.82.44.162

ip host windowserver1.capstone.local 10.82.44.164

ip host windowserver2.capstone.local 10.82.44.144

ip host windowserver1.capstone.local-rtp 10.82.44.164

ip host windowserver2.capstone.local-rtp 10.82.44.144

ip name-server 10.82.44.164 10.82.44.162

ip domain list linux.capstone.local

ip domain name capstone.local

!

ip dhcp pool wins1

utilization mark high 80 log

network 172.16.0.0 255.255.0.0

network 192.0.0.0 255.0.0.0 secondary

override default-router 192.1.0.0 255.0.0.0

override utilization high 60

override utilization low 40

bootfile xllboot

next-server 172.17.1.103 172.17.2.103

domain-name capstone.local

dns-server 10.100.0.251 10.82.44.164

netbios-name-server 172.16.1.103 172.16.2.103

netbios-node-type h-node

option 19 hex 01

lease 30

!mpls discovery vpn interval 3040

key chain to-r2

key 23

key-string 7 140732181F137A3920

crypto pki trustpoint TP-self-signed-3275798714

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-3275798714

revocation-check none

rsakeypair TP-self-signed-3275798714

!

crypto pki trustpoint SLA-TrustPoint

enrollment pkcs12

revocation-check crl

!

!

crypto pki certificate chain TP-self-signed-3275798714

crypto pki certificate chain SLA-TrustPoint

license udi pid CSR1000V sn 9J2TH7JSMUV

diagnostic bootup level minimal

memory free low-watermark processor 72314

!

!

et-analytics

!

spanning-tree extend system-id

!

username cal password 7 01030717481C091D25

username admin password 7 00141215174C04140B

username california password 7 021605481811003348

user-name ray

creation-time 1685717896

privilege 15

password 7 130B1606030D0A232E287D

class-map type inspect match-any Web\_app

match protocol tcp

match protocol udp

match protocol ftp

match protocol icmp

class-map type inspect match-all Web

match class-map Web\_app

match access-group name Web\_acl

!

policy-map type inspect INSIDE-OUTSIDE-POLICY

class type inspect Web

inspect

class class-default

drop log

!

zone security INSIDE

description Zone for inside interfaces

zone security OUTSIDE

description Zone for outside interfaces

zone security default

zone-pair security INSIDE-OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect INSIDE-OUTSIDE-POLICY

crypto map MY\_MAP 1 ipsec-isakmp

set peer 10.82.44.201

set transform-set MY\_SET

interface Loopback3

description loopback for eigrp advertisment

ip vrf forwarding 23

ip dhcp relay information trusted

ip address 3.3.3.3 255.255.255.0

ipv6 address FD01:ABAB::/64 eui-64

ipv6 address autoconfig

!

interface Port-channel23

description Connection to R2

ip vrf forwarding 23

ip address 192.168.123.3 255.255.255.0 secondary

ip address 192.168.23.3 255.255.255.0

interface Loopback3

description loopback for eigrp advertisment

ip vrf forwarding 23

ip dhcp relay information trusted

ip address 3.3.3.3 255.255.255.0

ipv6 address FD01:ABAB::/64 eui-64

ipv6 address autoconfig

!

interface Port-channel23

description Connection to R2

ip vrf forwarding 23

ip address 192.168.123.3 255.255.255.0 secondary

ip address 192.168.23.3 255.255.255.0

no negotiation auto

no mop enabled

no mop sysid

spanning-tree portfast

!

interface Tunnel10

no ip address

!

interface Tunnel20

no ip address

!

interface Tunnel50

no ip address

!

interface GigabitEthernet1

description r3 eth2 isp

ip address 192.168.1.10 255.255.255.0 secondary

ip address 192.168.23.3 255.255.255.0 secondary

ip address 10.82.44.202 255.255.255.248

ip nat inside

ip authentication mode eigrp 23 md5

ip authentication key-chain eigrp 23 to-r2

ip ospf 1 area 0

negotiation auto

ipv6 address FE80:: link-local

ipv6 address FD03::2:2/124

ipv6 enable

ipv6 ospf 1 area 0

no mop enabled

no mop sysid

crypto map MY\_MAP

!

interface GigabitEthernet2

description "Connection to R2"

ip address 10.82.44.226 255.255.255.248

ip nat inside

ip authentication mode eigrp 23 md5

ip authentication key-chain eigrp 23 to-r2

ip ospf 1 area 0

negotiation auto

ipv6 address FE80:: link-local

ipv6 address FD03::2:10/124

ipv6 address autoconfig

ipv6 enable

ipv6 ospf 1 area 0

no mop enabled

no mop sysid

crypto map MY\_MAP

!

interface GigabitEthernet3

description r3 eth7 lan

ip address 10.82.44.161 255.255.255.224

ip nat inside

ip ospf 1 area 0

negotiation auto

ipv6 address FD03::3:22/124

ipv6 address autoconfig

ipv6 enable

ipv6 ospf 1 area 0

no mop enabled

no mop sysid

!

!

router eigrp 23

network 0.0.0.0

!

router ospf 1

router-id 4.4.4.4

network 10.82.44.160 0.0.0.31 area 0

network 10.82.44.192 0.0.0.7 area 0

network 10.82.44.216 0.0.0.7 area 0

network 10.82.44.0 0.0.0.255 area 0

network 10.82.0.0 0.0.255.255 area 0

!

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

!

ip nat pool capstone 192.0.2.65 192.0.2.126 netmask 255.255.255.192

ip nat inside source list 1 pool capstone

ip route 0.0.0.0 0.0.0.0 10.82.44.201

ip route 192.0.2.128 255.255.255.224 GigabitEthernet1

ip ssh version 2

!

ip access-list extended Web\_acl

10 permit ip any any

!

ip access-list standard 1

40 permit 10.82.44.90

50 permit 10.82.44.66

20 permit 10.82.44.164

30 permit 10.82.44.144

10 permit 10.82.44.0 0.0.0.63

ip access-list standard 2

20 permit 10.82.44.90

10 permit 10.82.44.164

ip access-list standard 3

10 permit 192.168.0.0

20 permit 192.0.2.0

ip access-list standard 10

10 permit 10.82.44.0 0.0.0.31

20 permit 10.82.44.0 0.0.0.7

30 permit 10.100.0.0 0.0.0.255

ip access-list extended 100

10 permit ip host 10.82.44.161 host 10.82.44.129

20 permit ip host 10.82.44.161 host 10.82.44.25

30 permit ip host 10.82.44.161 host 10.82.44.65

ip access-list extended 101

10 permit udp any any eq domain

20 permit udp any eq domain any

ipv6 router ospf 1

!

!

control-plane

!

!

line con 0

password 7 03145A1815182E5E4A

stopbits 1

line vty 0 4

password 7 03145A1815182E5E4A

length 0

transport input ssh

!

!

end

## Linux Server Config

Last login: Mon Jun 5 09:11:51 2023 from 172.21.0.199

[ray@linux ~]$ testparm -v

Load smb config files from /etc/samba/smb.conf

Loaded services file OK.

Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE\_STANDALONE

Press enter to see a dump of your service definitions

# Global parameters

[global]

abort shutdown script =

add group script =

additional dns hostnames =

add machine script =

addport command =

addprinter command =

add share command =

add user script =

add user to group script =

afs token lifetime = 604800

afs username map =

aio max threads = 100

algorithmic rid base = 1000

allow dcerpc auth level connect = No

allow dns updates = secure only

allow insecure wide links = No

allow nt4 crypto = No

allow trusted domains = Yes

allow unsafe cluster upgrade = No

apply group policies = No

async dns timeout = 10

async smb echo handler = No

auth event notification = No

auto services =

binddns dir = /var/lib/samba/bind-dns

bind interfaces only = No

browse list = Yes

cache directory = /var/lib/samba

change notify = Yes

change share command =

check password script =

cldap port = 389

client ipc max protocol = default

client ipc min protocol = default

client ipc signing = default

client lanman auth = No

client ldap sasl wrapping = sign

client max protocol = default

client min protocol = SMB2\_02

client NTLMv2 auth = Yes

client plaintext auth = No

client protection = default

client schannel = Yes

client signing = default

client smb encrypt = default

client smb3 encryption algorithms = AES-128-GCM, AES-128-CCM, AES-256-GCM, AES-256-CCM

client smb3 signing algorithms = AES-128-GMAC, AES-128-CMAC, HMAC-SHA256

client use kerberos = desired

client use spnego principal = No

client use spnego = Yes

cluster addresses =

clustering = No

config backend = file

config file =

create krb5 conf = Yes

ctdbd socket =

ctdb locktime warn threshold = 0

ctdb timeout = 0

cups connection timeout = 30

cups encrypt = No

cups server =

dcerpc endpoint servers = epmapper, wkssvc, rpcecho, samr, netlogon, lsarpc, drsuapi, dssetup, unixinfo, browser, eventlog6, backupkey, dnsserver

deadtime = 10080

debug class = No

debug encryption = No

debug hires timestamp = Yes

debug pid = No

debug prefix timestamp = No

debug syslog format = No

winbind debug traceid = No

debug uid = No

dedicated keytab file =

default service =

defer sharing violations = Yes

delete group script =

deleteprinter command =

delete share command =

delete user from group script =

delete user script =

dgram port = 138

disable netbios = No

disable spoolss = No

dns forwarder =

dns port = 53

dns proxy = Yes

dns update command = /usr/sbin/samba\_dnsupdate

dns zone scavenging = No

dns zone transfer clients allow =

dns zone transfer clients deny =

domain logons = No

domain master = Auto

dos charset = CP850

dsdb event notification = No

dsdb group change notification = No

dsdb password event notification = No

enable asu support = No

enable core files = Yes

enable privileges = Yes

encrypt passwords = Yes

enhanced browsing = Yes

enumports command =

eventlog list =

get quota command =

getwd cache = Yes

gpo update command = /usr/sbin/samba-gpupdate

guest account = nobody

host msdfs = Yes

hostname lookups = No

idmap backend = tdb

idmap cache time = 604800

idmap gid =

idmap negative cache time = 120

idmap uid =

include system krb5 conf = Yes

init logon delay = 100

init logon delayed hosts =

interfaces =

iprint server =

kdc default domain supported enctypes = 0

kdc enable fast = Yes

kdc force enable rc4 weak session keys = No

kdc supported enctypes = 0

keepalive = 300

kerberos encryption types = all

kerberos method = default

kernel change notify = Yes

kpasswd port = 464

krb5 port = 88

lanman auth = No

large readwrite = Yes

ldap admin dn =

ldap connection timeout = 2

ldap debug level = 0

ldap debug threshold = 10

ldap delete dn = No

ldap deref = auto

ldap follow referral = Auto

ldap group suffix =

ldap idmap suffix =

ldap machine suffix =

ldap max anonymous request size = 256000

ldap max authenticated request size = 16777216

ldap max search request size = 256000

ldap page size = 1000

ldap passwd sync = no

ldap replication sleep = 1000

ldap server require strong auth = Yes

ldap ssl = start tls

ldap suffix =

ldap timeout = 15

ldap user suffix =

lm announce = Auto

lm interval = 60

load printers = Yes

local master = Yes

lock directory = /var/lib/samba/lock

lock spin time = 200

log file =

logging =

log level = 1

log nt token command =

logon drive =

logon home = \\%N\%U

logon path = \\%N\%U\profile

logon script =

log writeable files on exit = No

lpq cache time = 30

lsa over netlogon = No

machine password timeout = 604800

mangle prefix = 1

mangling method = hash2

map to guest = Never

max disk size = 0

max log size = 5000

max mux = 50

max open files = 16384

max smbd processes = 0

max stat cache size = 512

max ttl = 259200

max wins ttl = 518400

max xmit = 16644

mdns name = netbios

message command =

min domain uid = 1000

min receivefile size = 0

min wins ttl = 21600

mit kdc command =

multicast dns register = Yes

name cache timeout = 660

name resolve order = lmhosts wins host bcast

nbt client socket address = 0.0.0.0

nbt port = 137

ncalrpc dir = /run/samba/ncalrpc

netbios aliases =

netbios name = LINUX

netbios scope =

neutralize nt4 emulation = No

nmbd bind explicit broadcast = Yes

nsupdate command = /usr/bin/nsupdate -g

nt hash store = always

ntlm auth = ntlmv2-only

nt pipe support = Yes

ntp signd socket directory = /var/lib/samba/ntp\_signd

nt status support = Yes

null passwords = No

obey pam restrictions = No

old password allowed period = 60

oplock break wait time = 0

os2 driver map =

os level = 20

pam password change = No

panic action =

passdb backend = tdbsam

passdb expand explicit = No

passwd chat = \*new\*password\* %n\n \*new\*password\* %n\n \*changed\*

passwd chat debug = No

passwd chat timeout = 2

passwd program =

password hash gpg key ids =

password hash userPassword schemes =

password server = \*

perfcount module =

pid directory = /run

preferred master = Auto

prefork backoff increment = 10

prefork children = 4

prefork maximum backoff = 120

preload modules =

printcap cache time = 750

printcap name =

private dir = /var/lib/samba/private

raw NTLMv2 auth = No

read raw = Yes

realm =

registry shares = No

reject md5 clients = Yes

reject md5 servers = Yes

remote announce =

remote browse sync =

rename user script =

require strong key = Yes

reset on zero vc = No

restrict anonymous = 0

root directory =

rpc big endian = No

rpc server dynamic port range = 49152-65535

rpc server port = 0

rpc start on demand helpers = Yes

samba kcc command = /usr/sbin/samba\_kcc

security = USER

server max protocol = SMB3

server min protocol = NT1

server multi channel support = Yes

server role = auto

server schannel = Yes

server schannel require seal = Yes

server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl, winbindd, ntp\_signd, kcc, dnsupdate, dns

server signing = default

server smb3 encryption algorithms = AES-128-GCM, AES-128-CCM, AES-256-GCM, AES-256-CCM

server smb3 signing algorithms = AES-128-GMAC, AES-128-CMAC, HMAC-SHA256

server string = Samba 4.17.5

set primary group script =

set quota command =

show add printer wizard = Yes

shutdown script =

smb1 unix extensions = Yes

smb2 disable lock sequence checking = No

smb2 disable oplock break retry = No

smb2 leases = Yes

smb2 max credits = 8192

smb2 max read = 8388608

smb2 max trans = 8388608

smb2 max write = 8388608

smbd profiling level = off

smb passwd file = /var/lib/samba/private/smbpasswd

smb ports = 445 139

socket options = TCP\_NODELAY

spn update command = /usr/sbin/samba\_spnupdate

stat cache = Yes

state directory = /var/lib/samba

svcctl list =

syslog = 1

syslog only = No

template homedir = /home/%D/%U

template shell = /bin/false

time server = No

timestamp logs = Yes

tls cafile = tls/ca.pem

tls certfile = tls/cert.pem

tls crlfile =

tls dh params file =

tls enabled = Yes

tls keyfile = tls/key.pem

tls priority = NORMAL:-VERS-SSL3.0

tls verify peer = as\_strict\_as\_possible

unicode = Yes

unix charset = UTF-8

unix password sync = No

use mmap = Yes

username level = 0

username map =

username map cache time = 0

username map script =

usershare allow guests = No

usershare max shares = 0

usershare owner only = Yes

usershare path = /var/lib/samba/usershares

usershare prefix allow list =

usershare prefix deny list =

usershare template share =

utmp = No

utmp directory =

winbind cache time = 300

winbindd socket directory = /run/samba/winbindd

winbind enum groups = No

winbind enum users = No

winbind expand groups = 0

winbind max clients = 200

winbind max domain connections = 1

winbind nested groups = Yes

winbind normalize names = No

winbind nss info = template

winbind offline logon = No

winbind reconnect delay = 30

winbind refresh tickets = No

winbind request timeout = 60

winbind rpc only = No

winbind scan trusted domains = No

winbind sealed pipes = Yes

winbind separator = \

winbind use default domain = No

winbind use krb5 enterprise principals = Yes

wins hook =

wins proxy = No

wins server =

wins support = No

workgroup = SAMBA

write raw = Yes

wtmp directory =

idmap config \* : backend = tdb

access based share enum = No

acl allow execute always = No

acl check permissions = Yes

acl flag inherited canonicalization = Yes

acl group control = No

acl map full control = Yes

administrative share = No

admin users =

afs share = No

aio read size = 1

aio write behind =

aio write size = 1

allocation roundup size = 0

available = Yes

blocking locks = Yes

block size = 1024

browseable = Yes

case sensitive = Auto

check parent directory delete on close = No

comment =

copy =

create mask = 0744

csc policy = manual

cups options =

default case = lower

default devmode = Yes

delete readonly = No

delete veto files = No

dfree cache time = 0

dfree command =

directory mask = 0755

directory name cache size = 100

dmapi support = No

dont descend =

dos filemode = No

dos filetime resolution = No

dos filetimes = Yes

durable handles = Yes

ea support = Yes

fake directory create times = No

fake oplocks = No

follow symlinks = Yes

smbd force process locks = No

force create mode = 0000

force directory mode = 0000

force group =

force printername = No

force unknown acl user = No

force user =

fstype = NTFS

guest ok = No

guest only = No

hide dot files = Yes

hide files =

hide new files timeout = 0

hide special files = No

hide unreadable = No

hide unwriteable files = No

honor change notify privilege = No

hosts allow =

hosts deny =

include =

inherit acls = No

inherit owner = no

inherit permissions = No

invalid users =

kernel oplocks = No

kernel share modes = No

level2 oplocks = Yes

locking = Yes

lppause command =

lpq command = %p

lpresume command =

lprm command =

magic output =

magic script =

mangled names = illegal

mangling char = ~

map acl inherit = No

map archive = Yes

map hidden = No

map readonly = no

map system = No

max connections = 0

max print jobs = 1000

max reported print jobs = 0

min print space = 0

msdfs proxy =

msdfs root = No

msdfs shuffle referrals = No

nt acl support = Yes

ntvfs handler = unixuid, default

oplocks = Yes

path =

posix locking = Yes

postexec =

preexec =

preexec close = No

preserve case = Yes

printable = No

print command =

printer name =

printing = cups

printjob username = %U

print notify backchannel = No

queuepause command =

queueresume command =

read list =

read only = Yes

root postexec =

root preexec =

root preexec close = No

server smb encrypt = default

short preserve case = Yes

smbd async dosmode = No

smbd getinfo ask sharemode = Yes

smbd max async dosmode = 0

smbd max xattr size = 65536

smbd search ask sharemode = Yes

spotlight = No

spotlight backend = noindex

store dos attributes = Yes

strict allocate = No

strict locking = Auto

strict rename = No

strict sync = Yes

sync always = No

use client driver = No

use sendfile = No

valid users =

veto files =

veto oplock files =

vfs objects =

volume =

volume serial number = -1

wide links = No

write list =

[Share]

comment = Share File Server Share

path = /srv/samba/share

read only = No

valid users = @smbgrp

[Share1]

comment = Share File Server Share

force create mode = 0777

force directory mode = 0777

inherit permissions = Yes

path = /srv/samba/share1

read only = No

valid users = @smbgrp