Chapter 9 – Troubleshooting Converged Networks

Objectives

- Describe AAA operation & troubleshooting techniques.
- Describe the operation and configuration of classic and zone-based firewalls.
- Describe firewall troubleshooting techniques.
- Describe the operation and configuration of VPNs.
- Describe VPN troubleshooting techniques.

Security Implementation

- The implementation of security features can affect router and switch operation on different planes:
- *Management Plane:* Securing this plane is vital to the overall security of the device, as it allows access to device configuration via console, HTTP and VTY.
- *Control Plane:* represents all the functions and protocols that are used between network devices to control the operation of the network - such as routing protocols & STP.
- *Data Plane:* Routers and switches can inspect and filter traffic as part of the implementation of a security policy.

Management Plane Security

- Telnet transmissions contain unencrypted data (including the password), while SSH uses encryption to secure its transmission.

- The CLI can always be accessed through the serial console of the device. Authentication can limit access, but anyone with the ability to power cycle the device can perform the password recovery procedure and gain control of the device.

- Cisco Configuration Professional (CCP) or the Security Device Manager (SDM) can use either HTTP or HTTPS.

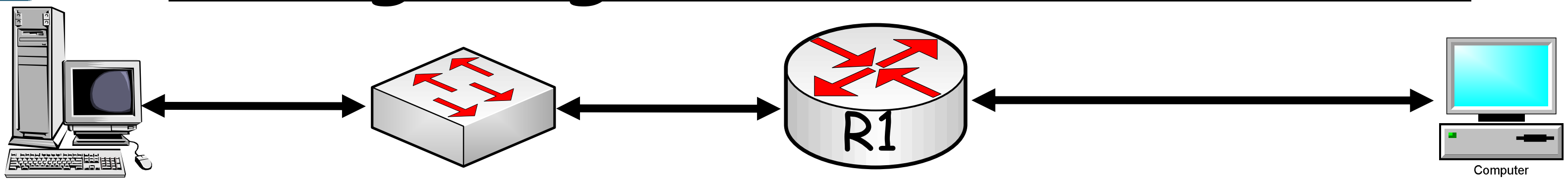
The Three Components of AAA

- *Authentication* - Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol selected, encryption . RADIUS combines authentication and authorisation, whereas TACACS+ decouples them.

- *Authorisation* - Provides the method for remote access control, including one-time authorisation or authorisation for each service. RADIUS does not allow specification (or enforcement) of which commands can be and which commands cannot be executed on a router, whereas TACAC+ does.

- *Accounting* - Provides the method for collecting and sending security server information used for billing, auditing, and reporting. RADIUS has extensive accounting capabilities, while TACACS+ has limited accounting capabilities.

Configuring AAA Authentication



AAA Server – 192.168.229.76

Configure TACAS+

R1(config)#aaa new-model
R1(config)#tacacs-server host 192.168.229.76 single-connection
R1(config)#tacacs-server key *ciscosecret*

Configure RADIUS

R1(config)#aaa new-model
R1(config)#radius-server host 192.168.229.76 auth-port 1812
R1(config)#radius-server key *ciscosecret*

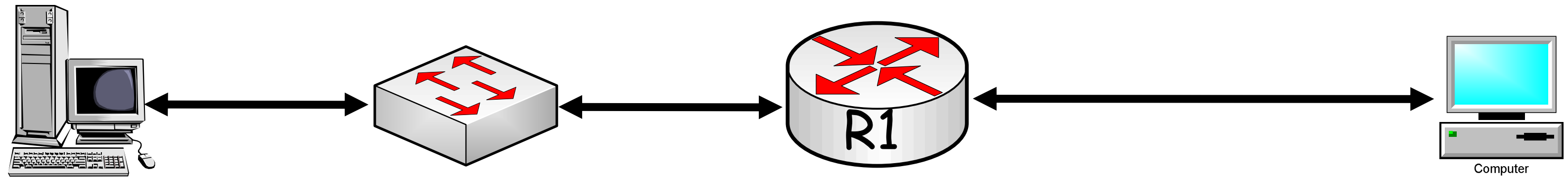
The authentication login command in global configuration mode enables the AAA authentication process:

1st 2nd 3rd

R1(config)#aaa authentication login default group radius local line
R1(config)#aaa authentication login TELNET_LINES group radius
R1(config)#line console 0
R1(config-line)#login authentication default
R1(config-line)#line vty 0 4
R1(config-line)#login authentication TELNET_LINES

R1#debug aaa authentication

'AAA Authorization' Commands



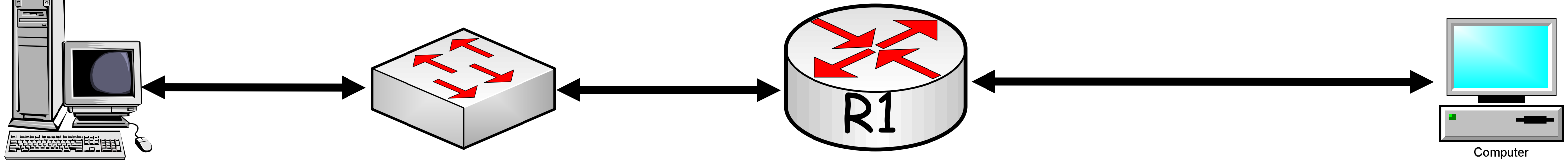
AAA Server –
192.168.229.76

R1(config)#aaa authorization exec default group radius local none

R1(config)#aaa authorization exec default group tacacs+ local none

R1#debug aaa authorization
R1#debug radius
R1#debug tacacs+

Configuring Local AAA Authentication/Authorisation

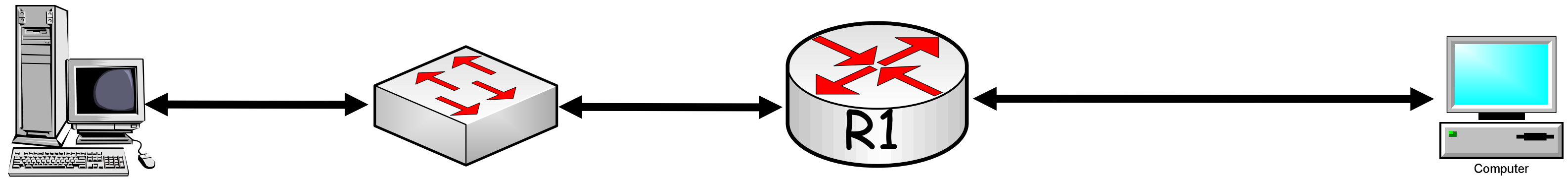


AAA Server – 192.168.229.76

R1(config)#username *admin* privilege 15 secret *cisco*
R1(config)#enable secret *class*
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
R1(config) #aaa authorization exec default local
R1(config)#line console 0
R1(config-line)#login local

- Authenticated user will still need to enter the 'enable secret' password to access privileged exec mode

AAA Accounting Commands



AAA Server –
192.168.229.76

R1(config)#aaa accounting exec default start-stop group radius

R1(config)#aaa accounting exec default stop-only group tacacs+

Only logs when an operation is completed – generates less information than the start-stop command

R1#debug aaa accounting

Troubleshooting the Management Plane

- From a troubleshooting standpoint, it is very important to know the answer to the following questions:

1. What security *policies* have been implemented for management access to the devices?
2. From which *IP addresses* or *networks* can the network devices be accessed?
3. What type of authentication, authorization, and accounting is used on the network?
4. If centralized AAA services are deployed, what happens when these servers fail or become *unreachable*?
5. Are there any *backdoors* or *fallback* mechanisms to access the devices?

Troubleshooting the Management Plane

R1#debug aaa authentication

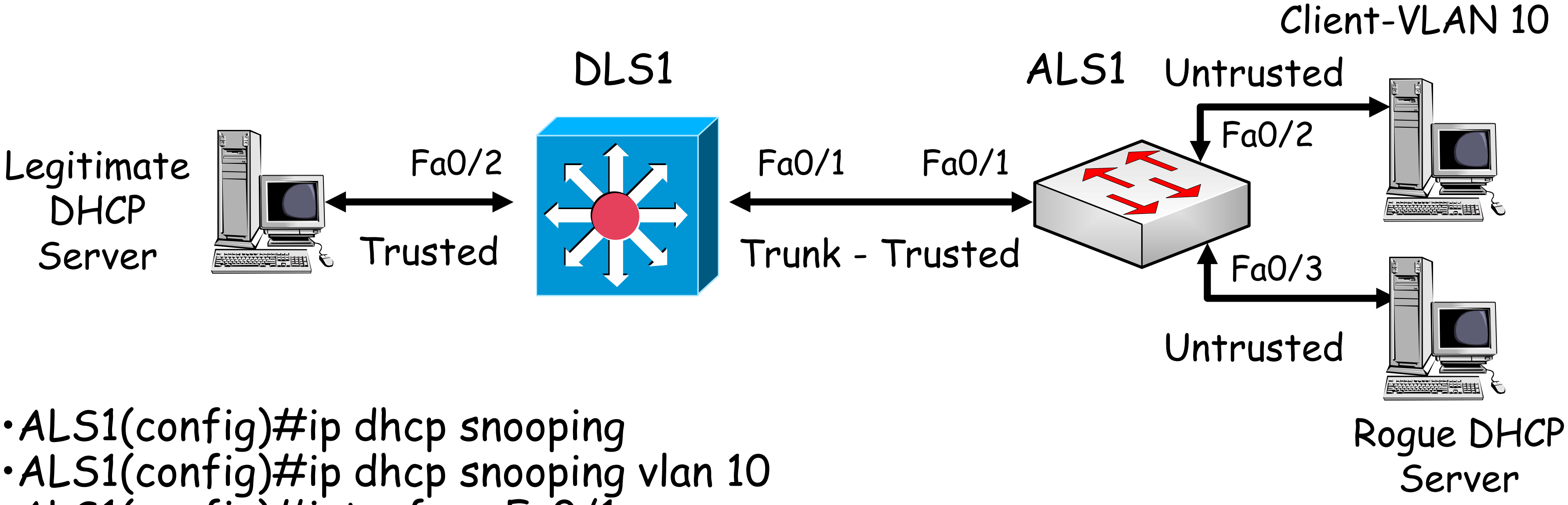
```
*Mar 3 14:39:39.435: AAA/BIND(0000000E): Bind i/f
*Mar 3 14:39:39.435: AAA/AUTHEN/LOGIN (0000000E): Pick method list 'ADMIN'
*Mar 3 14:39:59.211: AAA: parse name=tty66 idb type=-1 tty=-1
*Mar 3 14:39:59.211: AAA: name=tty66 flags=0x11 type=5 shelf=0 slot=0 adapter=0
port=66 channel=0
*Mar 3 14:39:59.211: AAA/MEMORY: create_user (0x83C938B4) user='kevin'
ruser='NULL' ds0=0 port='tty66' rem_addr='192.168.1.50' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
*Mar 3 14:39:59.211: AAA/AUTHEN/START (4286245615): port='tty66' list=''
action=LOGIN service=ENABLE
*Mar 3 14:39:59.211: AAA/AUTHEN/START (4286245615): non-console enable - default
to enable password
*Mar 3 14:39:59.215: AAA/AUTHEN/START (4286245615): Method=ENABLE
*Mar 3 14:39:59.215: AAA/AUTHEN(4286245615): Status=GETPASS
*Mar 3 14:40:00.710: AAA/AUTHEN/CONT (4286245615): continue_login
(user='(undef)')
*Mar 3 14:40:00.710: AAA/AUTHEN(4286245615): Status=GETPASS
*Mar 3 14:40:00.710: AAA/AUTHEN/CONT (4286245615): Method=ENABLE
*Mar 3 14:40:00.770: AAA/AUTHEN(4286245615): Status=PASS
*Mar 3 14:40:00.770: AAA/MEMORY: free_user (0x83C938B4) user='NULL' ruser='NULL'
port='tty66' rem_addr='192.168.1.50' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)
```

Troubleshooting the Control Plane

- A check-list similar to the following could be used by support engineers to troubleshoot control plane security implementations:

1. Are routing protocols or first hop redundancy protocols setup for *authentication* properly?
2. Are Spanning Tree Protocol security features such as BPDU Guard, BDPU Filter, Loop Guard, or Root Guard enabled correctly?
3. Is DHCP snooping configured properly?
4. Is the configuration of Dynamic ARP Inspection correct?
5. Are the configurations for control plane policing or control plane protection done *appropriately*?

DHCP Snooping - Configuration

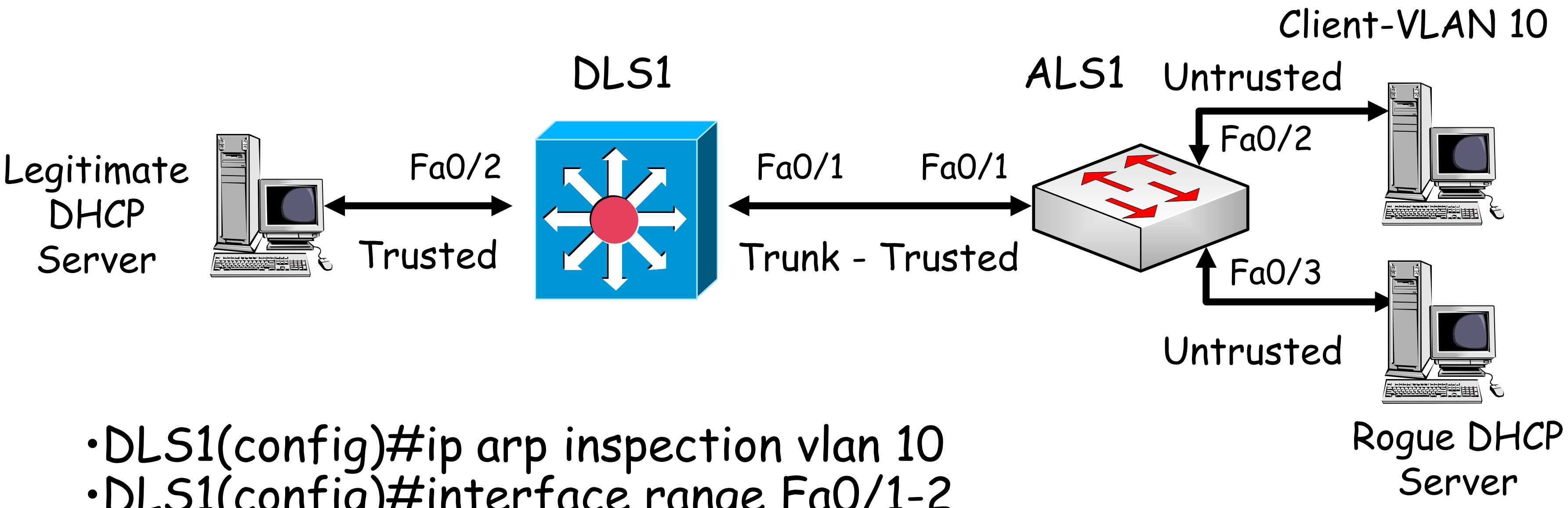


- ALS1(config)#ip dhcp snooping
- ALS1(config)#ip dhcp snooping vlan 10
- ALS1(config)#interface Fa0/1
- ALS1(config-if-range)#ip dhcp snooping trust
- ALS1(config)#interface range fa0/2-3
- ALS1(config-if-range)#ip dhcp snooping limit rate 20
- ALS1(config-if-range)#ip verify source vlan dhcp-snooping port-security

- DLS1(config)#ip dhcp snooping
- DLS1(config)#ip dhcp snooping vlan 10
- DLS1(config)#interface range Fa0/1-2
- DLS1(config-if-range)#ip dhcp snooping trust

- DLS1(config)# ip dhcp relay information trust-all

Dynamic ARP Inspection - Configuration

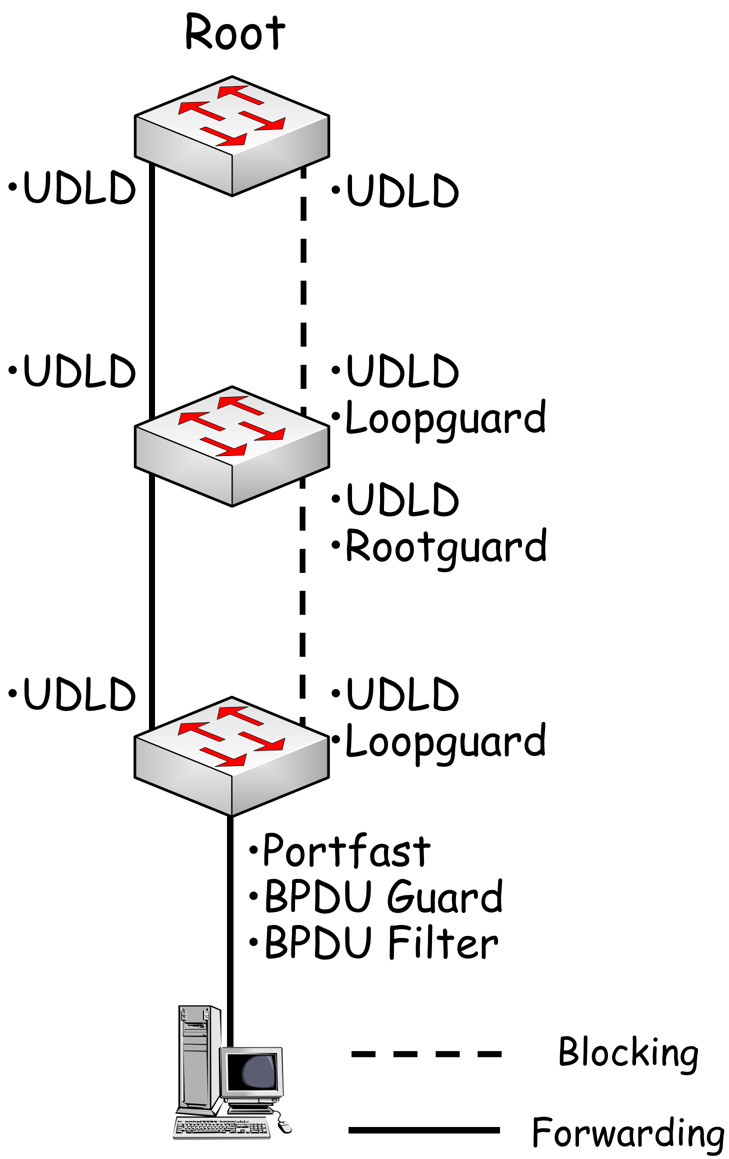


- DLS1(config)#ip arp inspection vlan 10
- DLS1(config)#interface range Fa0/1-2
- DLS1(config-if-range)#ip arp inspection trust

- ALS1(config)#ip arp inspection vlan 10
- ALS1(config)#ip arp inspection validate src-mac
- ALS1(config)#ip arp inspection validate dst-mac
- ALS1(config)#ip arp inspection validate ip

- ALS1(config)#interface Fa0/1
- ALS1(config-if-range)#ip arp inspection trust

Spanning Tree Protection



- Portfast – rapid transition to forwarding state for access ports.

- BPDU guard- protects portfast ports from creating loops.

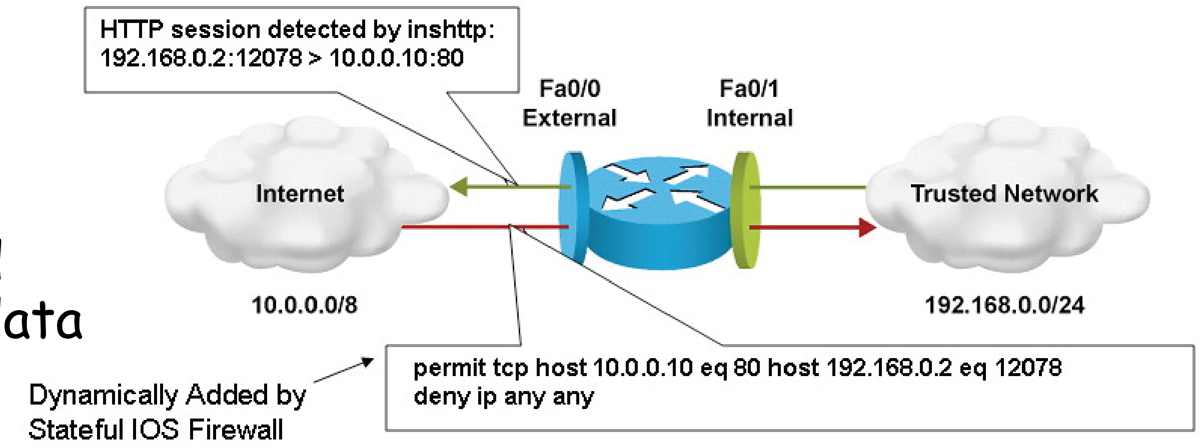
- BPDU Filter – stops BPDUs being sent from an interface.

- Root Guard – controls which ports are eligible to participate in root election.

- Unidirectional Link Detection (UDLD) – prevents links transitioning to forwarding state under unidirectional fault conditions.

- Loopguard – prevents links transitioning to forwarding under unidirectional fault conditions if designated port still operational.

Securing the Data Plane

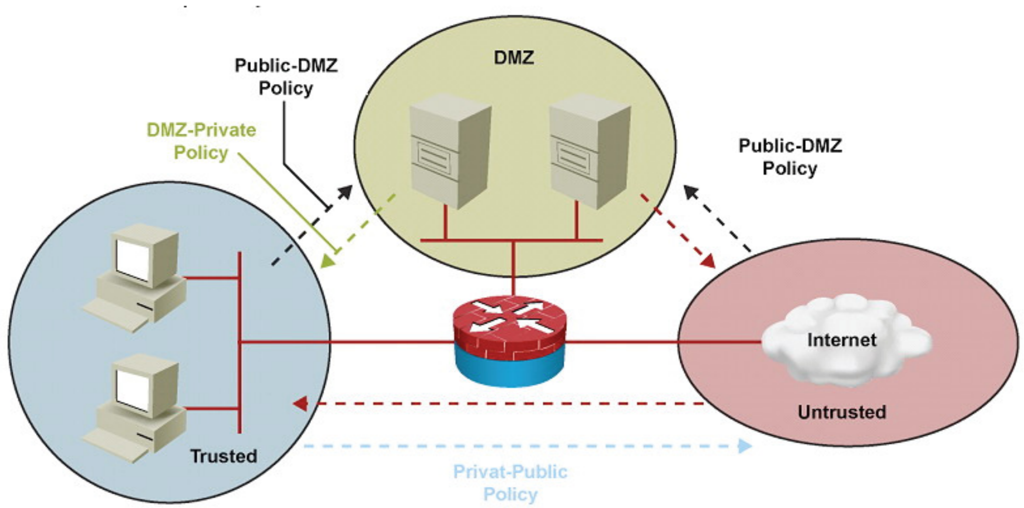


- The Cisco IOS Firewall software provides enhanced security functions for the data plane.

- There are two types of Cisco IOS Firewall:

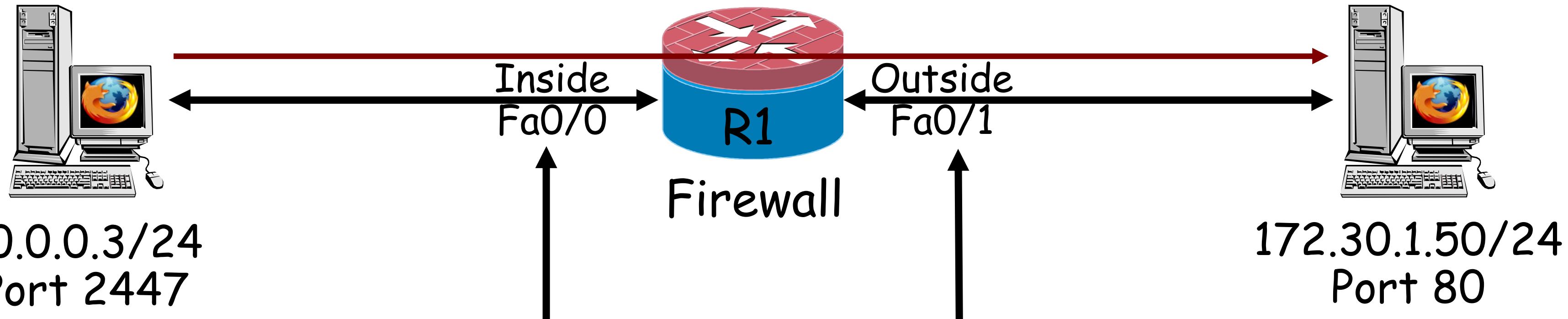
1. Classic Cisco IOS Firewall (stateful packet inspection)

2. Zone-Based Policy Firewall



Classic IOS Firewall Operation

1. Create Inspection rule and ACL:
Firewall(config)#ip inspect name FW_RULE tcp
Firewall(config)#access-list 101 permit tcp any any eq 80



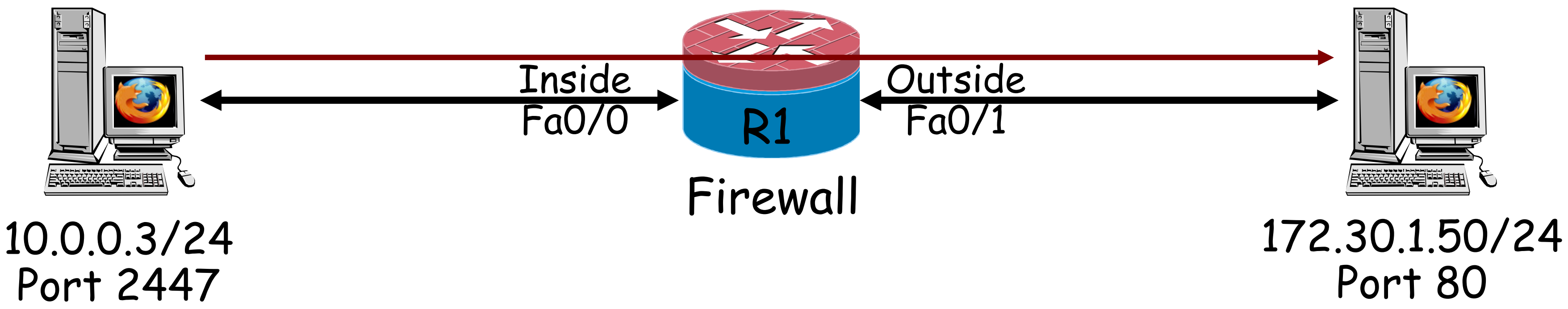
2. Apply Inspection rule and ACL to inside interface:
Firewall(config)# int fa0/0
Firewall(config-if)#ip access-group 101 in
Firewall(config-if)#ip inspect FW_RULE in

4. Apply ACL to outside interface:
Firewall(config)# int fa0/1
Firewall(config-if)#ip access-group 102 in

3. Create outside ACL:
Firewall(config)#access-list 102 deny ip any any
Firewall(config)#access-list 102 permit tcp 172.30.1.50 eq 80 host 10.0.0.3 eq 2447

Firewall#Show ip inspect config | session | interfaces

Verify Classic Firewall Operation



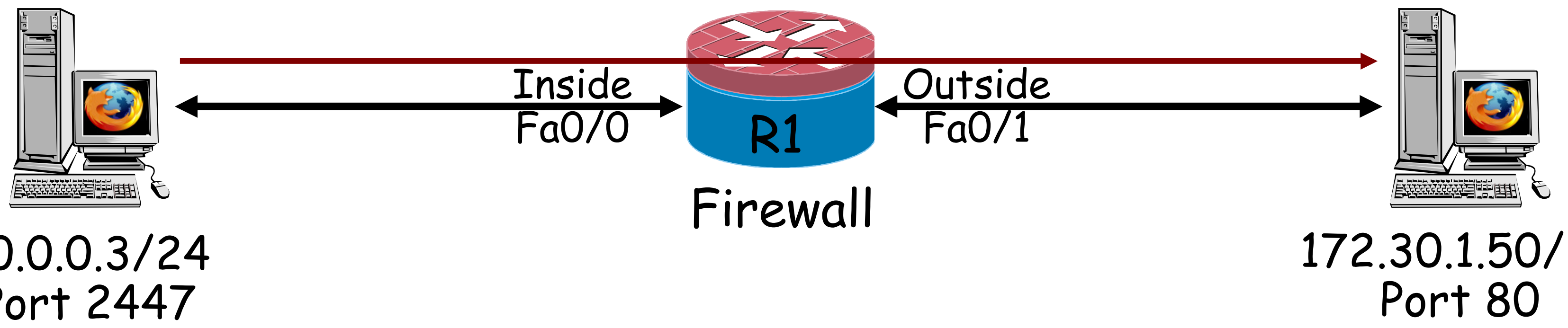
Firewall#**show ip inspect session**

Established Sessions

Session 84638E80 (10.0.0.3:2447)=>(172.30.1.50:80) http SIS_OPEN

Firewall#**show ip inspect session detail**
Established Sessions
Session 84638E80 (192.168.1.50:2447)=>(172.30.1.50:80) http SIS_OPEN
Created 00:01:54, Last heard 00:01:32
Bytes sent (initiator:responder) [408:166394]
In SID 172.30.1.50[80:80]=>10.0.0.3[2447:2447] on ACL 102 (116 matches)

Verify Classic Firewall Operation



Firewall#**show ip inspect all**

Session audit trail is enabled

Session alert is enabled

one-minute (sampling period) thresholds are [unlimited : unlimited] connections

max-incomplete sessions thresholds are [unlimited : unlimited]

max-incomplete tcp connections per host is unlimited. Block-time 0 minute.

tcp synwait-time is 30 sec — tcp finwait-time is 5 sec

tcp idle-time is 3600 sec — udp idle-time is 30 sec

tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo bytes

dns-timeout is 5 sec

Inspection Rule Configuration

Inspection name FW_RULE

http alert is on audit-trail is on timeout 3600

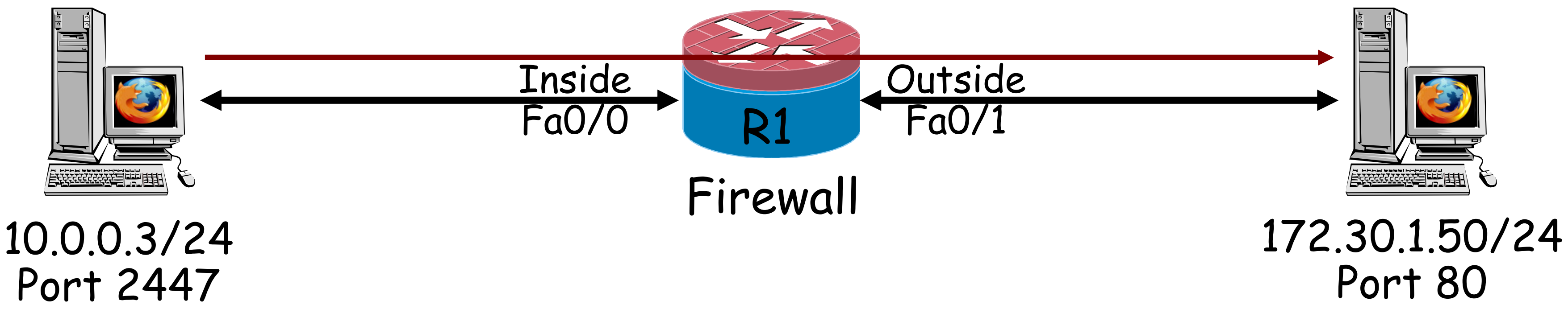
Interface Configuration

Interface FastEthernet0/0

Inbound inspection rule is FW_RULE

Outgoing inspection rule is not set

Monitor Classic Firewall Operation

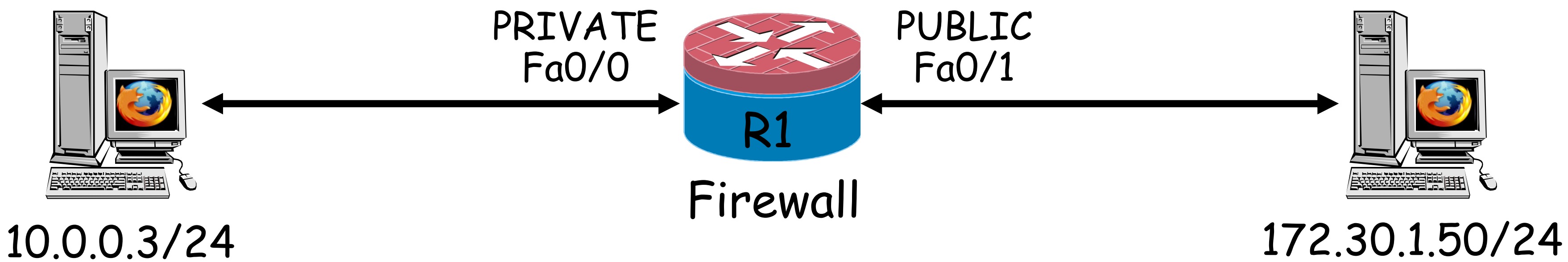


- To see real-time updates about the sessions being monitored by a router, enter the *ip inspect audit-trail* global configuration mode command.

- This causes syslog messages to be created whenever a router creates a new stateful inspection session.

Firewall(config)#**ip inspect audit-trail**
*Mar 3 12:46:32.465: %SYS-5-CONFIG_I: Configured from console by console
*Mar 3 12:47:10.115: %FW-6-SESS_AUDIT_TRAIL_START: Start http session: initiator (10.0.0.3:2447) — responder (172.30.1.50:80)

Zone Based Firewall Operation



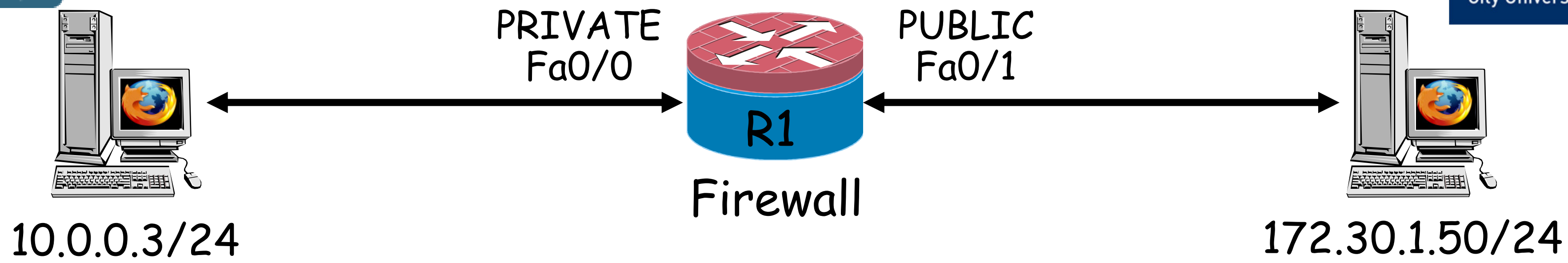

```
Firewall(config)#class-map type inspect match-any PRIV_PUB_CLASS
Firewall(config-cmap)#match prot http

Firewall(config)#policy-map type inspect PRIV_PUB_POL
Firewall(config-pmap)#class type inspect PRIV_PUB_CLASS
Firewall(config-pmap-c)#inspect

Firewall(config)#zone security PRIVATE
Firewall(config)#zone security PUBLIC

Firewall(config)#zone-pair security PRIV_PUB source PRIVATE destination PUBLIC
Firewall(config-sec-zone-pair)#service-policy type inspect PRIV_PUB_POL

Firewall(config)#int fa0/0
Firewall(config-if)#zone-member security PRIVATE
Firewall(config-if)#int fa0/1
Firewall(config-if)#zone-member security PUBLIC
```

Verify Zone Based Firewall Operation

- There are several useful show commands for performing Zone Based Policy Firewall troubleshooting and verification:

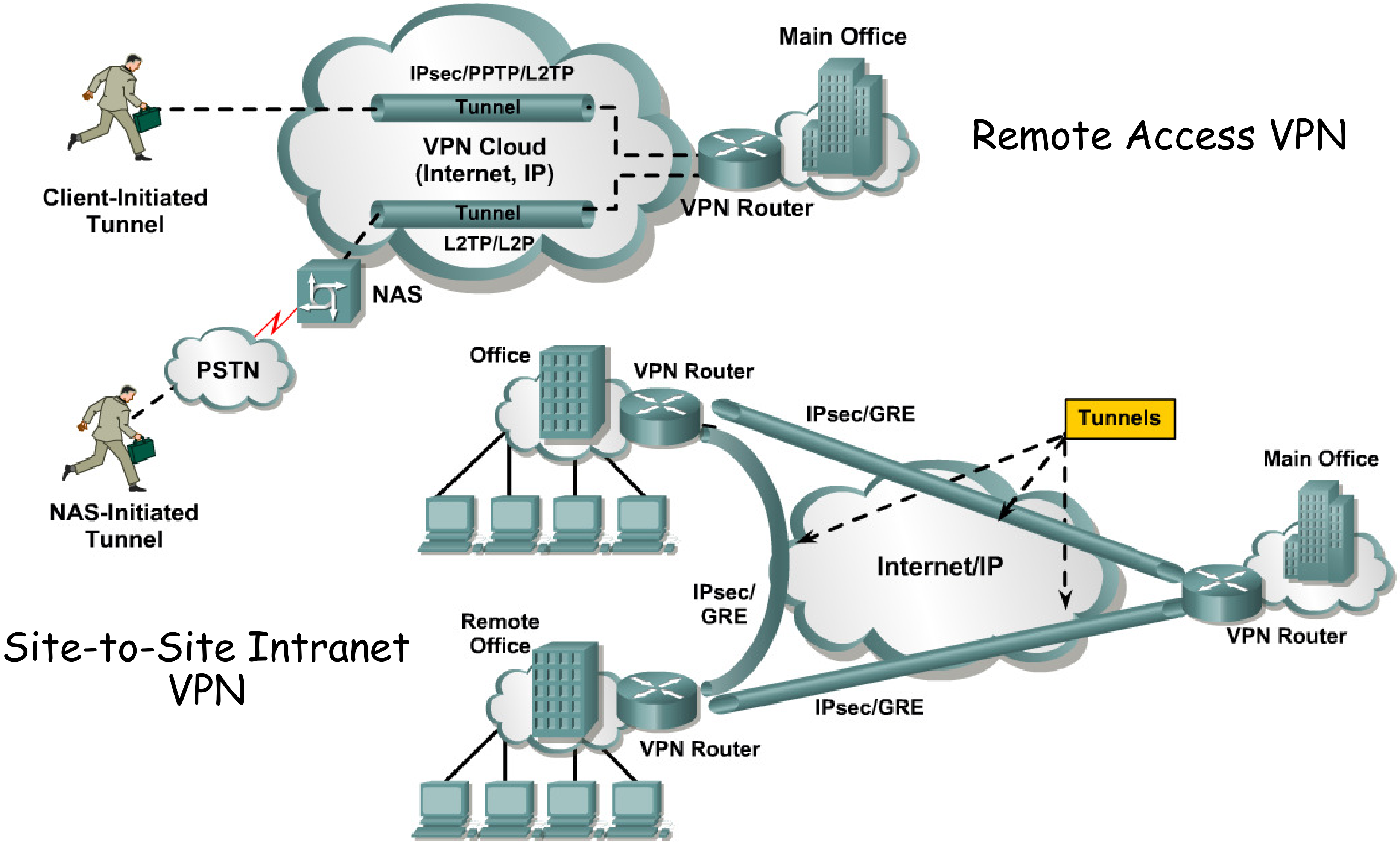
- *show zone security:* displays information for all the zones configured on the router and the corresponding member interfaces – allows verification of zones configuration and their assignment.
- *show zone-pair security:* provides important information about how zones are paired, the zone-pair direction (with respect to the traffic flow), and the policy applied to the zone-pair traffic.
- *show policy-map type inspect:* shows the relevant information for the policy, what traffic is matched to which class, and what action is applied to each class of traffic.

Firewall Exceptions




```
Firewall(config)# ip access-list extended INBOUND
Firewall(config-ext-nacl)#permit ahp host 172.30.1.50 host 10.0.0.3
Firewall(config-ext-nacl)#permit esp host 172.30.1.50 host 10.0.0.3
Firewall(config-ext-nacl)#permit gre host 172.30.1.50 host 10.0.0.3
Firewall(config-ext-nacl)#permit udp any any eq isakmp
Firewall(config-ext-nacl)#permit udp any any eq non500 isakmp
Firewall(config-ext-nacl)#permit icmp any any echo-reply
Firewall(config-ext-nacl)#permit icmp any any unreachable
Firewall(config-ext-nacl)#eigrp any any
Firewall(config)#int fa0/1
Firewall(config-if)#ip access-group INBOUND in
```

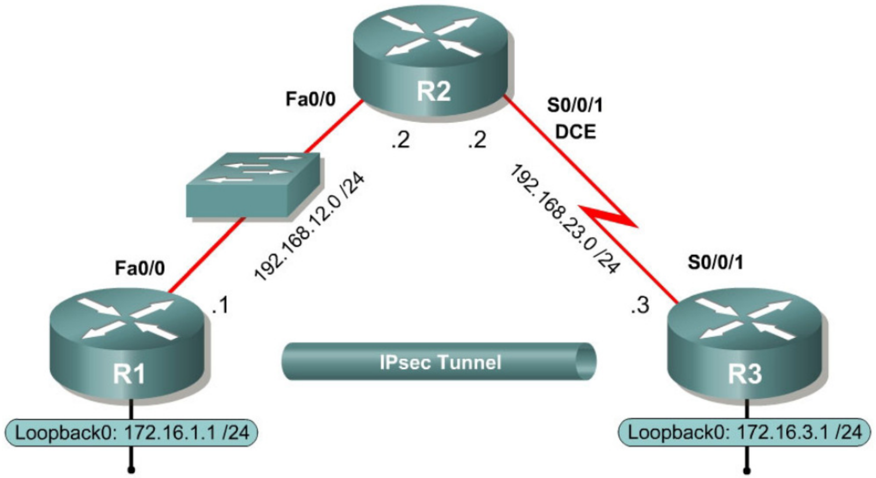
VPN Topologies



Remote Office Issues

- VPN mis-configuration.
- Over-lapping IP address spaces.
- Dynamic routing protocols, sub-optimal routing.
- MTU Size.
- Router processor overhead.
- User authentication.
- User software.

IPsec Tunnel CLI Configuration



R1(config)#crypto map VPN 10 ipsec-isakmp
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#set peer 192.168.23.3
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set transform-set 10

R1(config)#interface fa0/0
R1(config-if)#crypto-map *VPN*

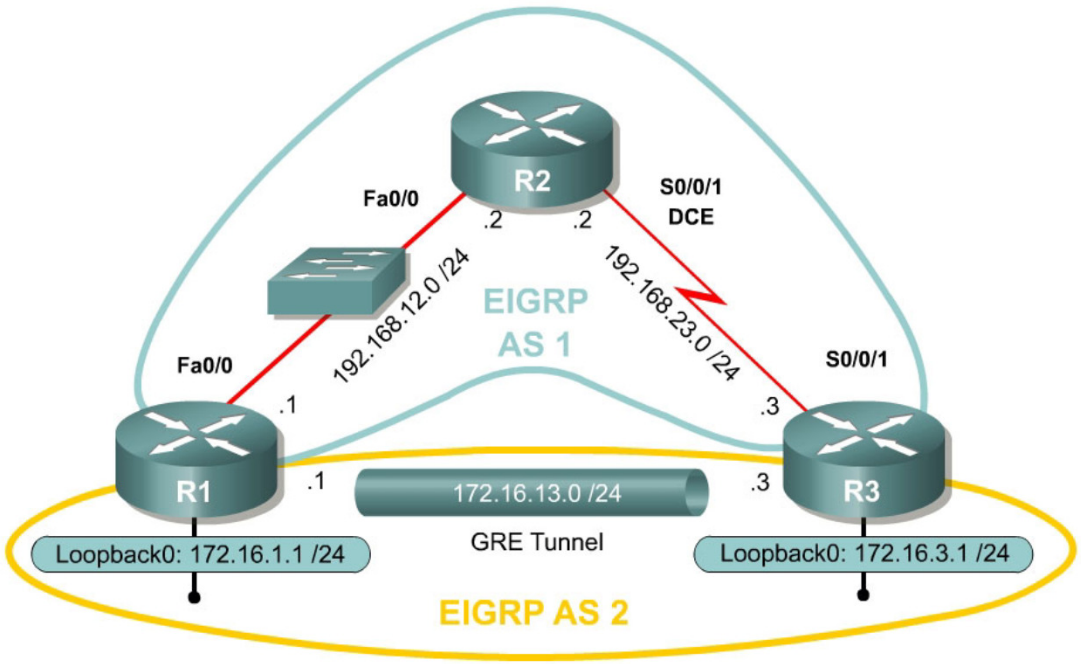
R1(config)# crypto isakmp policy *10*
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#hash sha
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config)#crypto isakmp key *cisco* address 192.168.23.3

R1(config)# crypto ipsec transform-set *10*
R1(cfg-crypto-trans)#esp-aes 256 esp-sha-hmac
R1(config)#crypto ipsec security-association lifetime seconds 1800

R1(config)#access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255

Secure GRE Tunnel CLI Configuration

Note - ISAKMP policy, IPsec transform sets & crypto maps must also be configured



R1(config)#interface tunnel 0
R1(config-if)#ip address 172.16.13.1 255.255.255.0
R1(config-if)#tunnel source fa0/0
R1(config-if)#tunnel destination 192.168.23.3

R1(config)#access-list 101 permit gre host 192.168.12.1 host 192.168.23.3

Note that this ACL must be 'mirrored' on R3 to reflect the difference in source and destination addresses.

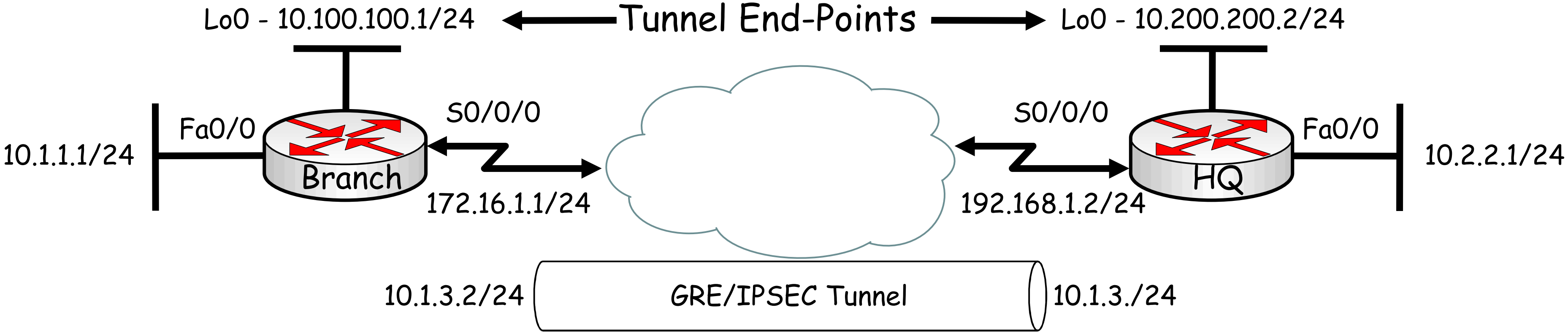
Verify VPN Service

- R1#show crypto ipsec sa
- R1#show crypto isakmp sa
- R1#show crypto session
- R1#show crypto map
- R1#debug crypto ipsec
- R1#debug crypto isakmp

```
R1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst            src            state      conn-id  slot  status
192.168.23.3   192.168.12.1   QM_IDLE    1002     0     ACTIVE
```

```
R1# show crypto map
Crypto Map "VPN" 10 ipsec-isakmp
Peer = 192.168.23.3
Extended IP access list 101
access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255
Current peer: 192.168.23.3
Security association lifetime: 4608000 kilobytes/1800 seconds
PFS (Y/N): N
Transform sets={
10,
}
Interfaces using crypto map map1:
FastEthernet0/0
```

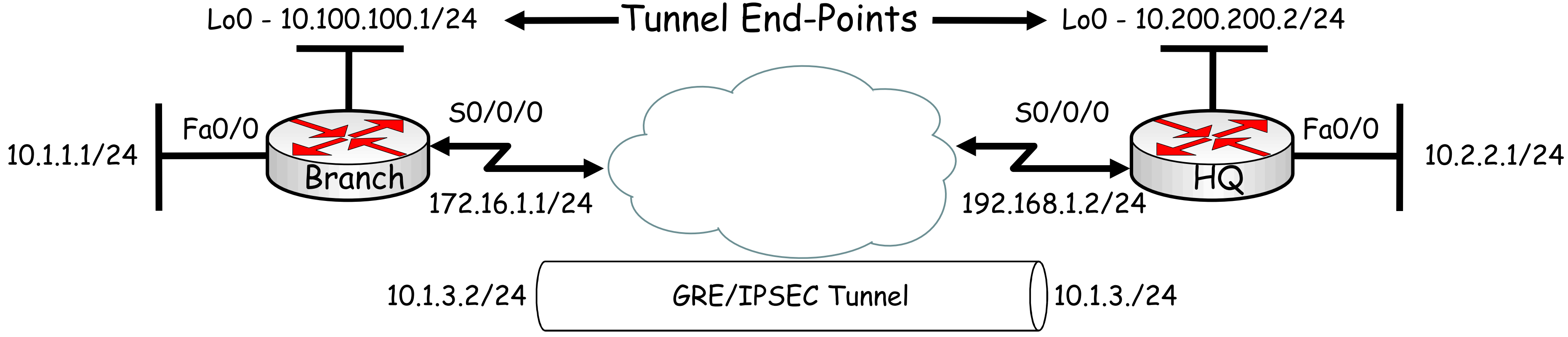
VPN Troubleshooting Example



•IPsec tunnel is established and tested, and it was carrying user traffic with no problem. Then tunnel interface went down and EIGRP was no longer able to advertise routes. Tunnels get established, only to go down after a few seconds every time.

BRANCH#**show interface tunnel0**
Tunnel0 is up, line protocol is down
Hardware is Tunnel
Internet address is 10.1.3.2 255.255.255.0
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
Reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.100.100.1 (Loopback101), destination 10.200.200.2
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled

VPN Troubleshooting Example



HQ(config)#**int tunnel0**

HQ(config-if)#**shutdown**

HQ(config-if)#**no shutdown**

HQ(config-if)#**end**

HQ#

%SYS-5-CONFIG_I: Configured from console by console

HQ#

%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.3.2 (Tunnel0) is up: new adjacency

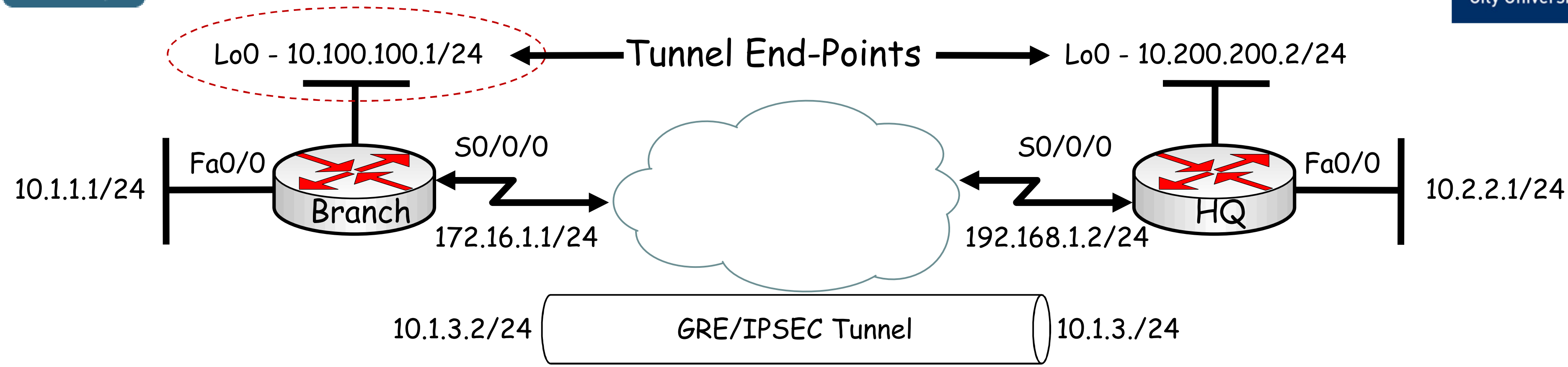
HQ#

%TUN-5-RECURDOWN: Tunnel0 temporarily disabled due to recursive routing

%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down

%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.3.2 (Tunnel0) is down: interface down

VPN Troubleshooting Example



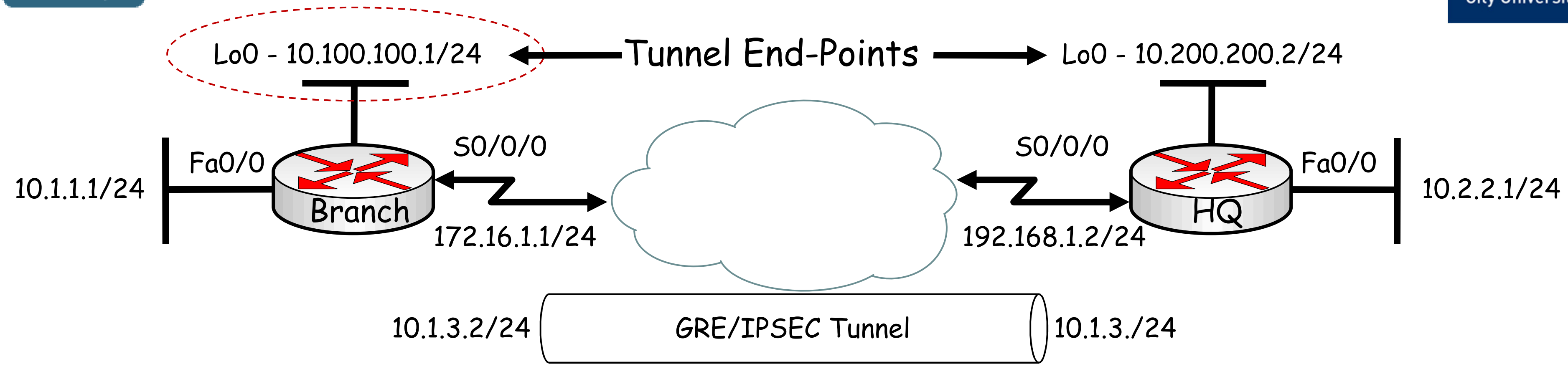
HQ# **show ip route**

10.0.0.0 255.0.0.0 is variably subnetted, 8 subnets, 2 masks

C 10.1.3.0 255.255.255.0 is directly connected, Tunnel0
C 10.200.200.0 255.255.255.0 is directly connected, Loopback0
D 10.100.100.0 255.255.255.0 [90/297372416] via 10.1.3.2, 00:00:07, Tunnel0
C 10.2.2.0 255.255.255.0 is directly connected, FastEthernet0/0
D 10.1.1.0 255.255.255.0 [90/297372416] via 10.1.3.2, 00:00:07, Tunnel0
C 192.168.1.0 255.255.255.0 is directly connected, serial0/0/0
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1

•Mis-configuration of routing over GRE tunnels can lead to recursive routing. When the ***best*** path to the ***tunnel destination*** is through the ***tunnel itself***, recursive routing causes the tunnel interface to flap.

VPN Troubleshooting Example



HQ (config)#**ip route 10.100.100.1 255.255.255.0 s0/0/0**
HQ# **show ip route**

10.0.0.0 255.0.0.0 is variably subnetted, 8 subnets, 2 masks
C 10.1.3.0 255.255.255.0 is directly connected, Tunnel0
C 10.200.200.0 255.255.255.0 is directly connected, Loopback101
D 10.100.100.0 255.255.255.0 [90/297372416] via 10.1.3.2, 00:00:07, Tunnel0
C 10.2.2.0 255.255.255.0 is directly connected, FastEthernet0/0
D 10.1.1.0 255.255.255.0 [90/297372416] via 10.1.3.2, 00:00:07, Tunnel0
S 10.100.100.1 255.255.255.255 [1/0] via 172.16.1.1
C 192.168.1.0 255.255.255.0 is directly connected, serial0/0/0
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1

•One way to fix this issue is to make sure that there is always a path to the tunnel destination, and that path is better than the one through the tunnel itself – use static routes.

Chapter 9 – Troubleshooting Converged Networks
Objectives

- Describe AAA operation & troubleshooting techniques.
- Describe the operation and configuration of classic and zone-based firewalls.
- Describe firewall troubleshooting techniques.
- Describe the operation and configuration of VPNs.
- Describe VPN troubleshooting techniques.

Any Questions?