SECURING COMPLEX NETWORKS REPORT

Zeo Motion
1405343@uad.ac.uk

1. Introduction

The purpose of this report is to show an understanding of complex networks, as well as how to defend such networks against potential threats. This report is split into 2 parts, with part one focusing on a site-to-site VPN and the defensive measures required, and part 2 focusing on securing an asterisk server to be used for VoIP. Details about configuration and any further information relating to each part can be found in the appendices at the end of this report.

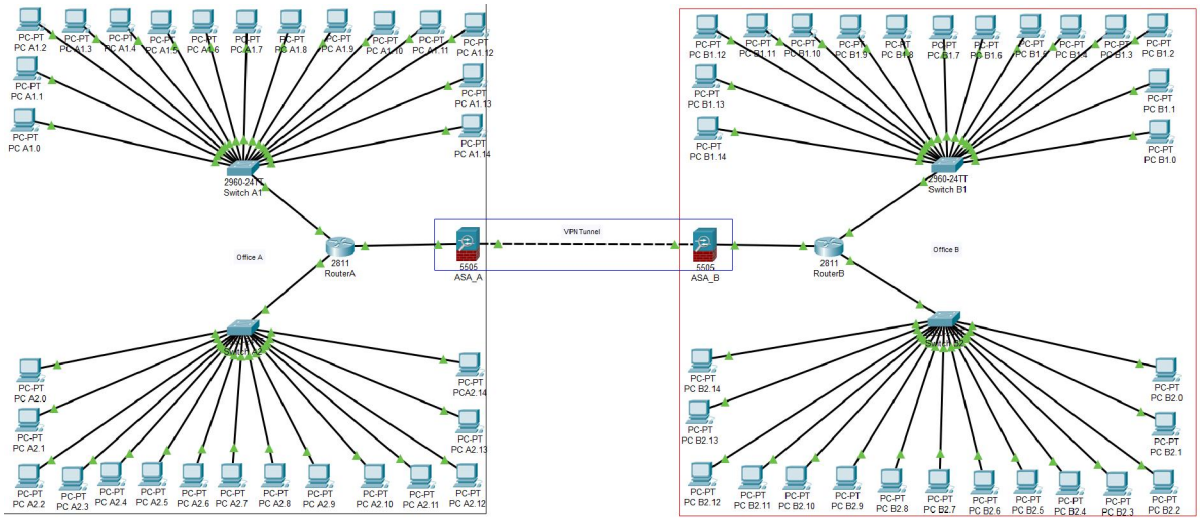
Github: https://github.com/Zeo445/PT1405343.git

2. Part 1

Part 1 of this assessment required the use of Cisco Packet Tracer to emulate a site-to-site VPN between 2 offices in different cities. Each of these offices were required to have 2 subnets with 15 pc's in each subnet (Totalling 30 in each office). It was also requested that RIPv2 was specifically used for the routing of the network.

2.1. Network

This section will detail the setup of part 1, detailing how each part was done and tested. Please note that the security aspects of setup will be discussed further in section 2.2.



2.1.1. Initial Setup

The initial setup was simple, first all the devices were placed in the offices (With the exception of the ASA firewalls). This was comprised of 2 sets of 15 computers per office connected to their respective routers via a switch. Following this the modules of each device were checked to ensure successful connection. Before any connections were established, passwords were set up on each router for each port (Refer to Part 1 appendix for list of password protected ports and their associated passwords). Once this was done the passwords were encrypted using the 'service password-encryption' command and the devices were then connected.

2.1.2. Subnetting and RIPv2

Each PC had their IP setup manually, as whilst this was a more difficult setup method it is more secure than dynamically assigning the IP via DHCP (PC IP list can be found in Part 1 appendix). Each PC was also assigned the netmask *255.255.255.128* as this signifies that there are 2 subnets in the network. Each PC was also told their respective gateway IPs as this was integral in allowing the subnets to communicate (xxx.xxx.xx.1 for the upper subnets and xxx.xxx.xx.192 for the lower subnets). The routers were set up so that the IP of the ports connected to each subnet corresponded to the correct gateway IP. The router IPs were also masked by the same netmask used on the PCs, and thus the networks were split into 2 subnets.

RIPv2 is a routing protocol that allows a router to keep track of the devices connected to it, however the advantage of this routing protocol specifically is that it can distinguish between different subnets. RIPv2 is easily configured by setting the version of rip on each router to *version 2* and specifying the network to be routed. Once the network was routed, a package was sent from one subnet to the other to test if the setup was successful.

2.1.3. VPN tunnel

There are 2 typical ways of connecting 2 networks via a VPN tunnel, either router-to-router or ASA 5505 to ASA 5505. I opted to go for the ASA method, as the ASA actively prevents any traffic from reaching the network during the setup, preventing malicious attacks mid-setup. Each ASA was placed on the edge of the network, and password protected to prevent potential malicious manipulation of configuration. Each ASA has 2 VLANs, one for the inner network and one for outside the network. The interface connected to the routers were set to VLAN 1 and assigned an IP, with the outer connection instead being connected to VLAN 2.

Each network IP and netmask were input as a network object for later sections of the VPN setup (Named OFFICE_A_NETWORK and OFFICE_B_NETWORK respectively). The access list was then altered to allow traffic between the 2 offices (both tcp and icmp traffic). The default routes for traffic inside and outside were then set, which required the destination IP, netmask and the gateway.

Next was the crypto map creation, which would allow the ASA to determine which traffic should be protected/allowed and how it goes about protecting said traffic. First a transform set was created named ‘L2L’. This set used aes as its encryption method as this is the most effective, and the set also used both hmac and sha for hashing (this is due to the ASA’s sharing a secret key). The maps were named ‘OFFICEA’ and ‘OFFICEB’ respectively, and were assigned the access list created previously. Next the peer IP for identification was input, followed by the transform set. The map was assigned to the outside interface. The ikev1 policy was then input, stating aes as the encryption, authentication to pre-share and the group to 2. Once all this was done, the tunnel group was set up as an ipsec-121 tunnel. The shared key “SHAREDSECRET” was then input.

2.2. Challenges faced

Throughout the creation of this network, there were many challenges faced, most of which could easily be solved:

1. PC’s from different subnets unable to communicate with each other

2. Continued failing of packet sending

3. VPN tunnel configured but not connecting

4. Unable to even send a packet through VPN tunnel

Another challenge was generally ensuring that the network was secure, which can often be a large undertaking.

2.2.1. Solutions/Downfalls

First, we'll discuss the previously mentioned challenges, detailing how they were or weren't solved.

1. This problem was caused by inputting the wrong IP on router A. Essentially the subnets were not connected where expected and therefore this problem was entirely due to human error.
2. Whilst this problem was caused by the IP mix up, packets still refused to successfully send unless PT was switched to 'Simulation' mode. Unsure what caused this issue.
3. This was a problem that no solution could be found for. Configuration was thoroughly checked on both ASA machines, and many online sources were reviewed but no irregularities or mismatches could be found that would cause this.
4. Once again this was likely caused by whatever caused the previous issue, but there were no indicators as to why this issue was occurring.

Securing a network is tricky at the best of times, in this case it was important to try to avoid any potential attacks during the set up as the network would be at its most vulnerable at this time. Both routers and ASA's had all possible passwords set with different passwords to ensure that they were as secure as possible, and the minimum password length of each device was set to 9 to ensure that if passwords need to be changed they will continue to be secure. As mentioned previously, the ASA devices act as a firewall, preventing anything that isn't whitelisted from accessing the network which greatly increases its security. The use of a shared key also means that nothing other than devices with the shared key can communicate with anything past the ASA, which could prevent malicious users from simply faking their IP to gain access (Spoofing) and could also prevent a malicious user altering the packets (Man-in-the-middle)

On the opposite however, there is still the potential for attacks to come through via means that cannot be fully protected, such as viruses sent via email. The ASA can be configured to single out the troubled device in this case, but this was not configured for this network.

3. Part 2

For this section of the assessment, we have been asked to allow two users to communicate via a VoIP ready asterisk server. We must ensure that the connection is adequately secure by setting up security and penetration testing the connection to find any potential vulnerabilities.

3.1. Configuration

In this section the setup and configuration of Asterisk is discussed.

3.1.1. AsteriskNow

To ensure a quick and easy installation, AsteriskNow was used as this handles much of the initial configuration and setup, and comes with freePBX which provides an easy to use GUI for the asterisk

server. During the setup, the user is given the option to provide a static IP which is recommended instead of allowing DHCP to assign the IP as a static IP does not change unless manually configured. The IP was set to 192.168.52.128.

3.1.2. FreePBX and SIP

Once The asterisk server was installed, another machine was used to access the FreePBX GUI. The Asterisk server was activated through this. Once Asterisk was activated, the GUI allowed activation of the included Sagoma Smart Firewall. The responsive firewall was setup for security (Discussed further in the next section). The 2 users were set up on freePBX via the extensions tab. The users were registered as 'friend1' with extension '1001' and 'friend2' with extension '1002'. Using the 'Zoiper' softphone, both users were connected to the asterisk server and a call was done to check the success of the setup. Call was successful.

3.2. Security

Security is essential for VoIP, as any matter of private information could be discussed via the internet. One benefit of using AsteriskNow is that a lot of the configuration defaults are surprisingly secure (some, not all). Strong passwords are one of the most common security aspects, and AsteriskNow automatically assigns a long and randomised password which would be impossible to brute force. The use of FreePBX also provided a simple to set up firewall, which included a responsive setting that would automatically block malicious attacks on the server, but would still allow access to trusted/registered users. Whilst these protect the server, the users must set up their own security on their end devices. Whilst it was not set up on this iteration, the Fail2Ban module can be used to prevent attackers from attempting to overuse the bandwith by setting a failed login limit. This should overall prevent attacks from occurring on the asterisk server.

3.3. Penetration Testing

The server was tested using Kali Linux and the SIPVicious penetration tools. Svmap was used first to determine if it could detect SIP on the network. Svmap managed to determine that SIP was enabled and showed the IP of the device. Next svwar was used to determine the extensions associated with this server. Whilst it was able to find the extensions, they both require authorisation which makes attempted cracking pointless. An attempt was made regardless, but knowing that there would likely be no end to the attempt it was stopped after a while.

As stated previously, it would be possible for SIPVicious to take up a largely unnecessary amount of bandwidth with constant attempts at password cracking. It is recommended that an automatic blacklist such as Fail2Ban is set up to prevent this from occurring. It is also recommended that the firewall is configured specifically to not allow anonymous calls, as this would be a relatively large security risk. Furthermore, it would be a good idea to ensure that only the ports essential to the running of asterisk are running to lessen the scope of vulernabilities. It may also be a good idea to block anonymous WAN requests altogether as advanced hackers may find a way to break in just by knowing the IP. It would also be a good idea to activate the "alwaysauthreject" configuration, as this makes it harder for SIP scanners to find valid extensions by rejecting certain authentication requests.

4. Conclusion

Network security is an essential part of networking, as without it our personal data would be constantly under risk. It is important to always ensure that as many steps as possible have been taken to ensure a secure and reliable network. Firewalls, port disabling, blacklists and whitelists, secure passwords, and most of all consistent and up to date networking knowledge are all essential when creating a complex network.

Appendices

This section contains the configuration files from both parts.

Part 1 appendix

Router A config

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 9
!
hostname RouterA
!
!
!
enable secret 5 $1$mERr$SqCBRQOLmhaH2foC0Z0uC/
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username infosec password 7 081259400F150A0017191F5379
!
!
!
!
!
!
!
```

```
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.10.129 255.255.255.128
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.128
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.20.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 192.168.10.0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
password 7 081544471A301636210E0F11382E14292026351C151251
login
!
line aux 0
password 7 08115E411D1802181C021F10737B
```

```
login
!
line vty 0 4
password 7 0807435C0C17161E11185B52
login
!
!
!
End
```

Router A passwords

Console: ThisIsASecurePassword2

Aux port: Protagonist90

VTY ports: Forensics76

Priv: Interfere555

Router B config

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 9
!
hostname RouterB
!
!
!
enable secret 5 $1$mERr$/Q5Hm0dt0/Ux4ls6O3hVq/
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username infosec password 7 0805455C1D0026181F1B19102F397D
!
!
!
!
!
```

```
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.30.1 255.255.255.128
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.30.129 255.255.255.128
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.20.2 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 192.168.30.0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
password 7 0803594C0B15001007065856
login
!
```

```
line aux 0
password 7 08125C4F0E11000306025B5D72
login
!
line vty 0 4
password 7 080A404B190D0A1A1305050578
login
!
!
!
end
```

Router B passwords

Console: Bubblegum42

Aux port: Spaghetti798

VTY ports: Kleptomania2

Priv: Introduction5

ASA A config

Password: NaNoWriMo67

```
ASA Version 8.4(2)
!
hostname ASA1
enable password 2RmkzhWAyIcwAs6c encrypted
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
```

```
security-level 100
ip address 192.168.10.1 255.255.255.128
!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.40.1 255.255.255.0
!
object network OFFICE_A_NETWORK
subnet 192.168.10.0 255.255.255.128
object network OFFICE_B_NETWORK
subnet 192.168.30.0 255.255.255.128
!
route outside 192.168.30.0 255.255.255.128 192.168.40.2 1
route inside 192.168.10.0 255.255.255.128 192.168.20.5 1
route inside 192.168.10.0 255.255.255.128 192.168.20.1 1
!
access-list OFFICE_B_TRAFFIC extended permit tcp object OFFICE_A_NETWORK object
OFFICE_B_NETWORK
access-list OFFICE_B_TRAFFIC extended permit icmp object OFFICE_A_NETWORK
object OFFICE_B_NETWORK
!
!
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
!
!
!
!
crypto ipsec ikev1 transform-set L2L esp-aes esp-sha-hmac
!
crypto map OFFICEB 1 match address OFFICE_B_TRAFFIC
crypto map OFFICEB 1 set peer 192.168.40.2
crypto map OFFICEB 1 set security-association lifetime seconds 86400
crypto map OFFICEB 1 set ikev1 transform-set L2L
crypto map OFFICEB interface outside
crypto ikev1 enable outside
crypto ikev1 policy 1
encr aes
authentication pre-share
```

```
group 2
!
tunnel-group 192.168.40.2 type ipsec-l2l
tunnel-group 192.168.40.2 ipsec-attributes
ikev1 pre-shared-key SHAREDSECRET
!
```

ASA B config

Password: Ult1matum03

```
ASA Version 8.4(2)
!
hostname ASA2
enable password 5n4KhhFmUIwzJBI5 encrypted
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.30.1 255.255.255.128
!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.40.2 255.255.255.0
!
object network OFFICE_A_NETWORK
subnet 192.168.10.0 255.255.255.128
object network OFFICE_B_NETWORK
subnet 192.168.30.0 255.255.255.128
!
route outside 192.168.10.0 255.255.255.128 192.168.40.1 1
route inside 192.168.30.0 255.255.255.128 192.168.20.2 1
!
```

```
access-list OFFICE_A_TRAFFIC extended permit tcp object OFFICE_B_NETWORK object
OFFICE_A_NETWORK
access-list OFFICE_A_TRAFFIC extended permit icmp object OFFICE_B_NETWORK
object OFFICE_A_NETWORK
!
!
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd enable inside
!
!
!
!
crypto ipsec ikev1 transform-set L2L esp-aes esp-sha-hmac
!
crypto map OFFICEA 1 match address OFFICE_A_TRAFFIC
crypto map OFFICEA 1 set peer 192.168.40.1
crypto map OFFICEA 1 set security-association lifetime seconds 86400
crypto map OFFICEA 1 set ikev1 transform-set L2L
crypto map OFFICEA interface outside
crypto ikev1 enable outside
crypto ikev1 policy 1
encr aes
authentication pre-share
group 2
!
tunnel-group 192.168.40.1 type ipsec-l2l
tunnel-group 192.168.40.1 ipsec-attributes
ikev1 pre-shared-key SHAREDSECRET
!
```

Part 2 appendix

```
accept_outofcall_message=yes
```

auth_message_requests=no

outofcall_message_context=dpma_message_context

faxdetect=no

vmexten=*97

useragent=FPBX-13.0.195.19(13.12.1)

language=en

disallow=all

allow=ulaw

allow=alaw

allow=gsm

allow=g726

context=from-sip-external

callerid=Unknown

notifyringing=yes

notifyhold=yes

tos_sip=cs3

tos_audio=ef

tos_video=af41

alwaysauthreject=yes

limitonpeers=yes

context=from-sip-external

callevents=yes

tcpenable=no

callerid=Unknown

bindport=5160

jbenable=no

allowguest=yes

srvlookup=no

defaultexpiry=120

minexpiry=60

maxexpiry=3600

```
g726nonstandard=no
videosupport=no
maxcallbitrate=384
canreinvite=no
rtptimeout=30
rtpholdtimeout=300
registerattempts=0
registertimeout=20
notifyhold=yes
notifyringing=yes
checkmwi=10
rtpkeepalive=0
nat=force_rport,comedia
ALLOW_SIP_ANON=no
tlsbindaddr=[::]:5161
tlscafile=/etc/pki/tls/certs/ca-bundle.crt
externip=92.239.68.107
localnet=192.168.52.0/24

!

#include pjsip.identify_custom.conf

[1001-identify]
type=identify
endpoint=1001

[1002-identify]
type=identify
endpoint=1002
```

!

#include pjsip.endpoint_custom.conf

[1001]

type=endpoint

aors=1001

auth=1001-auth

allow=ulaw,alaw,gsm,g726

context=from-internal

callerid=device <1001>

dtmf_mode=rfc4733

aggregate_mwi=yes

use_avpf=no

media_use_received_transport=no

trust_id_inbound=yes

media_encryption=no

timers=yes

media_encryption_optimistic=no

send_pai=yes

rtp_symmetric=yes

rewrite_contact=yes

force_rport=yes

language=en

[1001]

type=endpoint

aors=1002

auth=1002-auth

allow=ulaw,alaw,gsm,g726

context=from-internal

callerid=device <1002>

dtmf_mode=rfc4733

aggregate_mwi=yes

use_avpf=no

media_use_received_transport=no

trust_id_inbound=yes

media_encryption=no

timers=yes

media_encryption_optimistic=no

send_pai=yes

rtp_symmetric=yes

rewrite_contact=yes

force_rport=yes

language=en

[dpma_endpoint]

type=endpoint

context=dpma-invalid

!

#include pjsip.auth_custom.conf

[1001-auth]

type=auth

auth_type=userpass

password=c452f6bf4b711937fbfef76b2bfb402a

username=1001

[1002-auth]

type=auth

```
auth_type=userpass
password=h4k33foasn5340gs0083n451924ba94pi
username=1002

!

[modules]
autoload=yes
preload = pbx_config.so
preload = chan_local.so
preload = func_db.so
preload = res_odbc.so
preload = res_config_odbc.so
preload = cdr_adaptive_odbc.so
noload = chan_woomera.so
noload = pbx_gtkconsole.so
noload = pbx_kdeconsole.so
noload = app_intercom.so
noload = chan_modem.so
noload = chan_modem_bestdata.so
noload = chan_modem_i4l.so
noload = app_trunkisavail.so
noload = chan_alsa.so
noload = chan_oss.so
noload = app_directory_odbcstorage.so
noload = app_voicemail_odbcstorage.so
noload = chan_modem_aopen.so
noload = cdr_radius.so
noload = cel_radius.so
noload = cdr_mysql.so
noload = res_phoneprov.so
```

noload = res_config_ldap.so

noload = res_config_sqlite3.so

noload = res_clialiases.so

noload = chan_mgcp.so

noload = cdr_custom.so

noload = app_minivm.so

noload = cel_custom.so

load = format_wav.so

load = format_pcm.so

load = format_mp3.so

load = res_musiconhold.so