



Willie de Klerk

Student Number: 20230254

Student Year: 2 (2024)


MODULE: WIL620

Exit Level Outcome: 5

CTUTRAINING.AC.ZA | 0861 100 395 | ENQUIRY@CTUTRAINING.CO.ZA

Declaration of Authenticity

A critical aspect of any assignment is *authenticity*. Because you are completing much of the work for the assignments *unsupervised*, the examiner must be convinced that it is all your work. For this reason, you must complete the *Declaration of Authenticity* provided in the study guide and have it counter-signed by your manager, mentor, or lecturer.

	<p>The declaration of authenticity is a legal document, and if found that you have made a false declaration, then not only will your results be declared null and void, but you could also have criminal charges brought against you. It is not worth taking the risk!</p>
---	--

Please complete the declaration of authenticity below for all assignments:

DECLARATION OF AUTHENTICITY

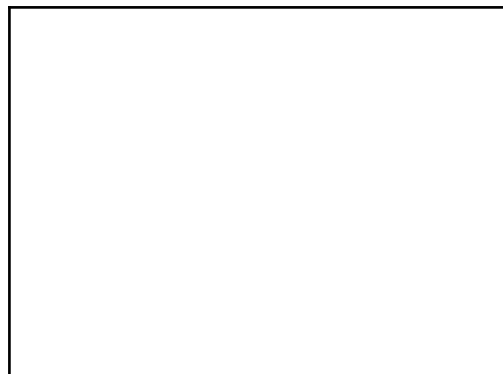


I WILLIE DE KLERK hereby

declare that the contents of this assignment are entirely my work except for the following documents:
(List the documents and page numbers of work in this portfolio that were generated in a group)

Activity	Date
Exit Level Outcome 5	2024/07/26

Signature:  Date: 2024/07/26



Company/Mentor Stamp

Contents

<i>Declaration of Authenticity</i>	1
Overview	3
Generic Routing Encapsulation (GRE):	3
IPsec	3
Risks associated with traffic traversing an untrusted network segment.....	3
Tapping.....	4
Tapping a fiber cable.....	4
Tapping experiment in a LAN environment.....	4
Some important context.....	7
Hash based Message Authentication Code.....	7
Advanced Encryption Standard (AES).....	7
Features of IPsec include.....	8
Packet Headers used by IPsec for packet delivery.....	8
IPsec transport modes.....	8
Transform Sets.....	9
Multiprotocol Label Switching (MPLS)	9
Label Switching.....	9
Label Bindings.....	10
Bibliography	10

Overview

Our data can take paths through virtual networks built on top of physical cabling and infrastructure. The virtual network and the tunnels can be seen as the overlay network whilst the physical hardware can be viewed as the underlay network.

With overlay technologies we can create a channel so that two different networks are able to communicate with each other across areas where destinations would not be directly routable. (We can create private networks across the internet)

The implementation of overlay networks are made possible through technologies such as:

- Generic Routing Encapsulation (GRE):
- IP Security (IPsec):
- Multiprotocol Label Switching (MPLS):

It is important to note that depending on the overlay technology being used, the data may not be encrypted, for example IPsec Supports encryption but GRE does not. Another key point to take note of is that MPLS tunneling is not supported when implementation across the internet is attempted, unless it is tunneled within a technology such as IPsec. MPLS over the internet: (Edgeworth, et al., 2019)

Generic Routing Encapsulation (GRE):

GRE is a tunneling protocol that supports encapsulation of generic protocols within an IPv4 packet header. This means that you can encapsulate protocols such as IPv6, MPLS, IPv4 or other protocols that have an IPv4 packet header with a GRE tunnel.

Implementation of GRE tunnels take place in 7 steps:

1. Create the tunnel interface
2. Identify the source of the tunnel, meaning what will be encapsulated and de-encapsulated. An example would be traffic from a specific physical interface.
3. Identifying the remote destination IP address and setting it as the destination address.
4. Allocating an IP address to the tunnel interface.
5. If specificity is needed the tunnel bandwidth should be defined.
6. If the tunnel destination is not in the routing table a gre keepalive should be specified.
7. Optionally a maximum transmission unit (MTU) value should be specified for the tunnel interface.

Generic Routing Encapsulation (GRE) Tunnels: (Edgeworth, et al., 2019)

IPsec

IPsec is a framework of open standards that allow for the creation of secure virtual private networks.

Risks associated with traffic traversing an untrusted network segment.

While there are technologies in place to ensure that application data sent over the internet is encrypted such as https (Hypertext Transfer Protocol Secure), it does not however perform packet encryption to ensure that the source and destination IP address of the IP of the traffic is secured.

This would still be dangerous since if someone was able to figure out what website you are frequently visiting, they would be able to create a fake website and try to obtain information such as your credentials. This attack usually fools mostly non tech savvy company employees. An example where this information would be valuable would be when someone is using online banking.

Tapping

Tapping a fiber cable

A fiber cable used to provide internet to a business can be easily tapped by the use of a fiber optic splitter that can split the light across a prism. With this implementation the original stream would stay intact and a second stream can be sent to a traffic analyzer.

Whilst the traffic analyzer would not be able to see the individual computers on the other side of the router due to the implementation of NAT (Network Address Translation), it would still be able to see what resources the devices on the other side are most frequently accessing through the router. By analyzing the traffic a lot can be learned about the business and their employee habits.

The equipment involved to execute this is quite expensive but it can be obtained if attacking a business is the goal. The most expensive would be the splicing tool used to add connectors to the fiber cable that has been cut.

Tapping experiment in a LAN environment

For this experiment I am making use of a Cisco Catalyst c3650 switch to replicate the traffic. I am implementing Switched Port Analyzer (SPAN) technologies, more specifically I am making use of the Local Switched Port Analyzer Technique to capture traffic generated on the port on which my computer is connected to and I am sending the traffic to a raspberry pi on another port running a terminal based version of Wireshark known as [tshark](#). I will have a capture for normal traffic as well as a capture for when I use IPsec on my computer.



Switch Setup

```
Switch(config)#monitor session 1 source interface gigabitEthernet 1/0/3
Switch(config)#monitor session 1 destination interface gigabitEthernet 1/0/2
```

On the switch gi 1/0/1 will be my uplink. Interface gi 1/0/3 will be used by my computer. Interface gi 1/0/2 will be used by the raspberry pi.

```
Switch#show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
    Both            : Gi1/0/3
Destination Ports   : Gi1/0/2
Encapsulation       : Native
    Ingress         : Disabled
```

As mentioned previously I am using the Local Switched Port Analyzer technique.

Looking at non IPsec traffic

In this section a glance will be taken at the traffic captured while IPsec is not being used. I generated the traffic by browsing the evetech.co.za website.

```
▼ Queries
  ▼ evetech.co.za: type A, class IN
    Name: evetech.co.za
    [Name Length: 13]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
  ▼ Answers
    ▶ evetech.co.za: type A, class IN, addr 104.26.13.248
    ▶ evetech.co.za: type A, class IN, addr 172.67.68.103
    ▶ evetech.co.za: type A, class IN, addr 104.26.12.248
    [Request In: 488]
    [Time: 0.011004103 seconds]
```

Whilst this will not be visible when a solution as DoH (DNS over HTTPS) I could see the dns request as well. This gave me the IP address that is used to communicate with the evetech server. If DoH or Quic is being used for DNS queries,

I would have to rely on techniques such as nslookup to resolve the hostname. This would require a PTR record to perform the reverse dns request ([rdns](#)). If there are no PTR DNS records setup for the website I will not be able perform the reverse lookup. Taking on the mind of an attacker I would most likely run a script to do this trying to resolve the IP addresses captured.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
3.161.94.127	1				0.0001	0.10%	0.0100	2.453
95.100.108.145	1				0.0001	0.10%	0.0100	9.744
95.100.108.219	1				0.0001	0.10%	0.0100	5.865
13.107.21.237	2				0.0002	0.20%	0.0200	2.242
204.79.197.203	2				0.0002	0.20%	0.0200	2.241
52.111.240.3	2				0.0002	0.20%	0.0200	3.305
192.168.0.13	4				0.0004	0.40%	0.0200	9.050
204.79.197.219	4				0.0004	0.40%	0.0200	2.242
172.67.74.152	10				0.0010	1.01%	0.0700	3.605
13.245.194.131	11				0.0011	1.11%	0.1100	3.615
159.89.102.253	12				0.0012	1.21%	0.0300	3.954
52.85.254.126	12				0.0012	1.21%	0.1200	5.638
142.251.47.138	13				0.0013	1.31%	0.1000	3.293
216.239.38.181	13				0.0013	1.31%	0.0400	3.700
51.132.193.105	13				0.0013	1.31%	0.1200	3.374
192.178.54.99	19				0.0019	1.92%	0.1100	3.714
3.161.94.22	19				0.0019	1.92%	0.0900	4.251
192.178.54.42	25				0.0025	2.52%	0.0800	4.364
142.251.47.131	28				0.0029	2.83%	0.1100	3.483
192.178.54.100	38				0.0039	3.83%	0.1100	2.412
52.183.220.149	38				0.0039	3.83%	0.1300	1.879
208.67.222.222	91				0.0093	9.18%	0.4500	3.156
172.67.68.103	124				0.0126	12.51%	0.5400	3.540
192.168.0.23	504				0.0513	50.86%	0.9600	3.524
Destination IPv4 Addresses 991					0.1009	100%	1.9700	3.524
108.181.120.239	1				0.0001	0.10%	0.0100	1.648
13.107.21.237	1				0.0001	0.10%	0.0100	2.235
13.107.21.239	1				0.0001	0.10%	0.0100	6.017
20.250.77.142	1				0.0001	0.10%	0.0100	0.237
204.79.197.203	1				0.0001	0.10%	0.0100	2.235
95.100.108.145	1				0.0001	0.10%	0.0100	9.720
95.100.108.219	1				0.0001	0.10%	0.0100	5.842
3.161.94.127	2				0.0002	0.20%	0.0100	2.235
204.79.197.219	3				0.0003	0.30%	0.0200	2.235
224.0.0.251	3				0.0003	0.30%	0.0300	9.038
52.111.240.3	3				0.0003	0.30%	0.0100	2.235
192.168.0.13	4				0.0004	0.40%	0.0200	1.906
51.132.193.105	8				0.0008	0.81%	0.0500	3.206
13.245.194.131	9				0.0009	0.91%	0.0900	3.590
216.239.38.181	9				0.0009	0.91%	0.0300	3.524
159.89.102.253	11				0.0011	1.11%	0.0300	3.957
52.85.254.126	11				0.0011	1.11%	0.1100	5.633
142.251.47.138	12				0.0012	1.21%	0.0600	3.200
172.67.74.152	12				0.0012	1.21%	0.1000	3.599
192.178.54.99	15				0.0015	1.51%	0.0800	3.722
3.161.94.22	16				0.0016	1.61%	0.0800	3.293
192.178.54.42	19				0.0019	1.92%	0.0700	4.364
142.251.47.131	26				0.0026	2.62%	0.0800	3.402
192.178.54.100	26				0.0026	2.62%	0.0900	2.412
52.183.220.149	95				0.0097	9.59%	0.4300	1.879
172.67.68.103	108				0.0110	10.90%	0.5800	3.149
208.67.222.222	108				0.0110	10.90%	0.5800	3.149
192.168.0.23	484				0.0493	48.84%	1.0200	3.530

Looking at the destination IPv4 addresses I found the address used for evetech. Following that I added a filter to Wireshark to filter based on that IP address being in the traffic, either as source or destination. The application data between my computer and evetech is encrypted using (TLSv1.3).

ip.addr == 172.67.68.103							
No.	Time	Source	Destination	Protocol	Length	Info	
235	3.195492674	192.168.0.23	172.67.68.103	TLSv1.3	2080	Client Hello	
260	3.204361717	172.67.68.103	192.168.0.23	TLSv1.3	1429	Server Hello, Change Cipher Spec, Application Data	
264	3.205475679	192.168.0.23	172.67.68.103	TLSv1.3	118	Change Cipher Spec, Application Data	
282	3.212057787	172.67.68.103	192.168.0.23	TLSv1.3	566	Application Data, Application Data	
350	3.358386077	192.168.0.23	172.67.68.103	TLSv1.3	146	Application Data	
351	3.358737381	192.168.0.23	172.67.68.103	TLSv1.3	85	Application Data	
352	3.358737693	192.168.0.23	172.67.68.103	TLSv1.3	685	Application Data	
353	3.358737901	192.168.0.23	172.67.68.103	TLSv1.3	162	Application Data	
354	3.358738110	192.168.0.23	172.67.68.103	TLSv1.3	171	Application Data	
361	3.362874166	172.67.68.103	192.168.0.23	TLSv1.3	85	Application Data	
398	3.435059688	172.67.68.103	192.168.0.23	TLSv1.3	758	Application Data	
400	3.448496664	172.67.68.103	192.168.0.23	TLSv1.3	356	Application Data	
402	3.451185528	172.67.68.103	192.168.0.23	TLSv1.3	357	Application Data	
404	3.453294130	192.168.0.23	172.67.68.103	TLSv1.3	125	Application Data	
428	3.536034794	192.168.0.23	172.67.68.103	TLSv1.3	197	Application Data	
429	3.536035054	192.168.0.23	172.67.68.103	TLSv1.3	132	Application Data	
430	3.536035211	192.168.0.23	172.67.68.103	TLSv1.3	132	Application Data	
431	3.536035419	192.168.0.23	172.67.68.103	TLSv1.3	134	Application Data	
432	3.536035627	192.168.0.23	172.67.68.103	TLSv1.3	93	Application Data	
433	3.536035784	192.168.0.23	172.67.68.103	TLSv1.3	93	Application Data	
434	3.536036044	192.168.0.23	172.67.68.103	TLSv1.3	93	Application Data	
435	3.536079221	192.168.0.23	172.67.68.103	TLSv1.3	94	Application Data	
438	3.536460993	192.168.0.23	172.67.68.103	TLSv1.3	157	Application Data	

Although the data is encrypted, I know the IP address of the destination node. Once again taking on the role of an attacker I could create a phishing website hosted on a similar domain, with an appearance of the evetech website or a banking website. I could send emails to the respective company employees to get them to click on a link for my domain. Once again this is a concern if people are using online banking or entering their details in a checkout section.

Looking at IPsec Traffic

In this section a glance will be taken at IPsec traffic that has been encrypted making use of the ESP (Encapsulating Security Payload) header for packet delivery. ESP will be discussed during the section of IPsec Headers. With this being implemented, only the IP address of the destination of the IPsec tunnel is visible and not the IP address of the website that is being visited.

No.	Time	Source	Destination	Protocol	Length	Info
12	0.671363339	192.168.0.23	197.242.155.197	ESP	142	ESP (SPI=0xc0e3968f)
13	0.671612602	192.168.0.23	197.242.155.197	ESP	142	ESP (SPI=0xc0e3968f)
14	0.680562227	197.242.155.197	192.168.0.23	ESP	186	ESP (SPI=0x3d726ddc)
15	0.682013016	192.168.0.23	197.242.155.197	ESP	130	ESP (SPI=0xc0e3968f)
16	0.683280322	192.168.0.23	197.242.155.197	ESP	146	ESP (SPI=0xc0e3968f)
17	0.689555340	197.242.155.197	192.168.0.23	ESP	130	ESP (SPI=0x3d726ddc)
18	0.690033398	192.168.0.23	197.242.155.197	ESP	118	ESP (SPI=0xc0e3968f)
19	0.690777542	192.168.0.23	197.242.155.197	ESP	1478	ESP (SPI=0xc0e3968f)
20	0.690777647	192.168.0.23	197.242.155.197	ESP	750	ESP (SPI=0xc0e3968f)
21	0.694704403	197.242.155.197	192.168.0.23	ESP	210	ESP (SPI=0x3d726ddc)
22	0.696665593	197.242.155.197	192.168.0.23	ESP	118	ESP (SPI=0x3d726ddc)
23	0.697199223	192.168.0.23	197.242.155.197	ESP	130	ESP (SPI=0xc0e3968f)
24	0.697199327	192.168.0.23	197.242.155.197	ESP	762	ESP (SPI=0xc0e3968f)
25	0.697199431	192.168.0.23	197.242.155.197	ESP	762	ESP (SPI=0xc0e3968f)
26	0.698237264	192.168.0.23	197.242.155.197	ESP	146	ESP (SPI=0xc0e3968f)
27	0.702775148	197.242.155.197	192.168.0.23	ESP	130	ESP (SPI=0x3d726ddc)
28	0.703318829	192.168.0.23	197.242.155.197	ESP	118	ESP (SPI=0xc0e3968f)
29	0.704078598	192.168.0.23	197.242.155.197	ESP	1478	ESP (SPI=0xc0e3968f)
30	0.704078702	192.168.0.23	197.242.155.197	ESP	738	ESP (SPI=0xc0e3968f)
31	0.709988783	197.242.155.197	192.168.0.23	ESP	118	ESP (SPI=0x3d726ddc)
32	0.709988888	197.242.155.197	192.168.0.23	ESP	118	ESP (SPI=0x3d726ddc)
33	0.714157043	197.242.155.197	192.168.0.23	ESP	1478	ESP (SPI=0x3d726ddc)
34	0.714157199	197.242.155.197	192.168.0.23	ESP	134	ESP (SPI=0x3d726ddc)

This is in essence a brick wall for any attacker trying to gain access to company traffic and the habits of the employees at the site. An attacker will be able to do nothing other than frown and possibly cry, going to their home in shame having wasted all their time and money learning nothing about the company.

Some important context

To better understand the features and functionality included with IPsec some time should be given to understanding the fundamental difference between HMAC and encryption using AES.

Hash based Message Authentication Code

HMAC is a type of message authentication code that is obtained through the execution of a cryptographic hash function on data to allow for authentication and shared key. HMAC's implementation is used for data integrity and authentication.

HMACs provide parties with a unique shared private key that is known only to them. The client makes a unique hash (HMAC) for every request. When the client sends a request to the server it hashes the requested data with a private key separately and sends it as part of the request.

When the server receives the request it makes its own HMAC. The HMACs generated are compared and if both are equal, the client is considered legitimate. (www.geeksforgeeks.org, 2024)

Advanced Encryption Standard (AES)

AES is a specification for the encryption of electronic data. Older encryption algorithms include DES and triple DES, however they are no longer in use due to AES offering stronger encryption.

AES is a block cipher. AES works by performing a series of linked operations which involves replacing and shuffling input data. Data is encrypted in blocks rather than bits.

Depending on the size of the encryption key, the amount of times the process of shuffling and replacement of input data will take place differs. The larger the key the more shuffling will take place. (www.geeksforgeeks.org, 2023)

Features of IPsec include

- Peer authentication: The identity of the peer is verified through authentication methods such as a pre-shared key.
- Data confidentiality: Data is encrypted, ensuring confidentiality via encryption algorithms and encryption standards such as AES.
- Data integrity: Data integrity is ensured through hashing algorithms such as SHA-1.
- Replay detection: Every packet is uniquely marked via a sequence number.

Packet Headers used by IPsec for packet delivery

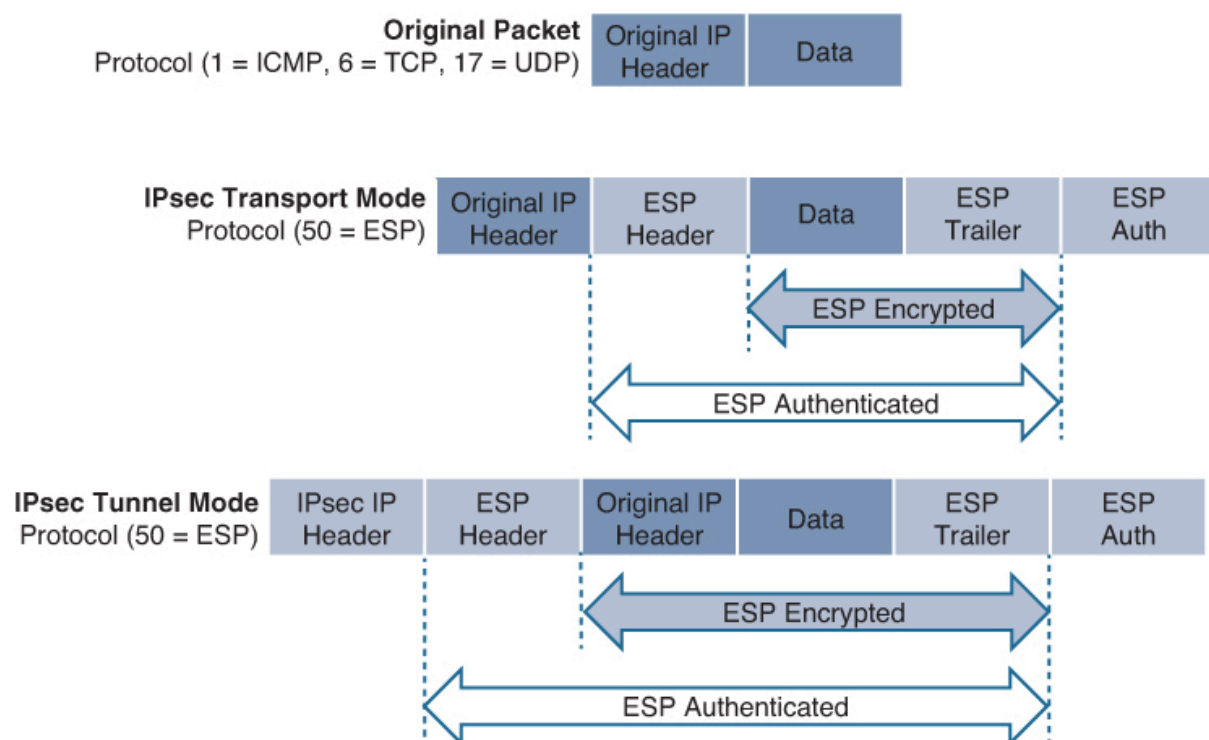
Authentication header: The authentication header does not support encryption however it provides data integrity and authentication. Its use is not recommended unless authentication is all that is desired.

Encapsulating Security Payload (ESP): The ESP header provides data confidentiality, authentication, and protection from replay attacks. ESP encrypts the original payload (before encapsulation) adding new headers for transport over the public network.

IPsec transport modes

Tunnel Mode: packet based encryption as well as the addition of new IPsec headers to route the packet and provide overlay functionality.

Transport mode: Payload based encryption and authentication without new IPsec headers or support for overlay functions.



Transform Sets

During IPsec Security Association negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

Transform types include:

- Authentication header transform (only 1 allowed)
- ESP encryption transform (only one allowed)
- ESP authentication transform (only one allowed)
- IP compression transform.

Internet Key Exchange (IKE):

- A protocol that performs authentication between two endpoints to establish security associations (SAs), also known as IKE tunnels.
- The security associations are used to carry control plane and data plane traffic for IPsec.
- There are two versions: IKEv1 and IKEv2.
 - IKEv1 is still important since it is supported by legacy infrastructure.

IPsec Fundamentals (Edgeworth, et al., 2019)

Multiprotocol Label Switching (MPLS)

- MPLS combines the performance capabilities of Layer 2 switching with the scalability of Layer 3 routing.
- MPLS allows efficient delivery of IP services of ATM switched networks.
- MPLS supports the creation of routes between source and destinations on a purely router-based Internet Backbone.

Label Switching



With a normal Layer 3 forwarding mechanism a packet will traverse the network and at each router along the line extracts the information needed to forward the packet from the Layer 3 header. The extracted information is used as an index for the routing table lookup to determine the next hop for the packet.

Usually speaking, the dst header field is the only relevant bit of information needed from the Layer 3 header. In some cases other header fields are relevant. Thus in normal layer 3 forwarding mechanisms the header should be inspected independently and table lookups should also take place at each hop.

With the implementation of label switching, the layer 3 header inspection is only done once. After the inspection is performed the layer 3 header is then mapped into a fixed length, unstructured value called a label. (32-bit Shim Header contains the 20 bit label)



Headers can be mapped into the same label as long as the next hop is always the same. A label represents a set of packets no matter how different they are, and cannot be viewed differently in terms of forwarding.

At subsequent hops through each MPLS router in each network, labels are swapped and forwarding decisions are made by means of MPLS forwarding table lookups for the label carried in the packet header. MPLS forwarding table lookups are faster than conventional layer 3 lookups.

Label Bindings

Each Label Switching Router makes their own decision to determine a label value to represent a forwarding equivalence class resulting in a label binding. Neighbours are informed of these label bindings that have been made. Label values change as packets traverse the network.

MPLS Basic MPLS Configuration Guide (www.cisco.com, 2013)

Bibliography

Edgeworth, B., Rios, R. G., Gooley, J. & Hucaby, D., 2019. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide | Chapter 16 //Section 3. [Online] Available at: <https://learning.oreilly.com/library/view/ccnp-andccie/9780135262047/ch16.xhtml#ch16lev1sec3> [Accessed 28 06 2024].

Edgeworth, B., Rios, R. G., Gooley, J. & Hucaby, D., 2019. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide | Chapter 16 //Section 4. [Online] Available at: <https://learning.oreilly.com/library/view/ccnp-andccie/9780135262047/ch16.xhtml#ch16lev1sec4> [Accessed 28 06 2024].

Edgeworth, B., Rios, R. G., Gooley, J. & Hucaby, D., 2019. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide | Chapter 16. Overlay Tunnels Intro. [Online] Available at: <https://learning.oreilly.com/library/view/ccnp-andccie/9780135262047/ch16.xhtml#:text=MPLS%20tunneling%20is,another%20overlay%20tunnel>. [Accessed 28 06 2024].
www.cisco.com, 2013.

MPLS Basic MPLS Configuration Guide. [Online] Available at: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/mp_basic/configuration/xe-16/mp-basic-xe-16-book.pdf [Accessed 28 06 2024]. www.geeksforgeeks.org, 2023. Advanced Encryption Standard (AES). [Online] Available at: <https://www.geeksforgeeks.org/advanced-encryption-standard-aes/> [Accessed 28 06 2024].
www.geeksforgeeks.org, 2024.

What is HMAC (Hash Based Message Authentication Code)?. [Online] Available at: <https://www.geeksforgeeks.org/what-is-hmachash-based-messageauthentication-code/> [Accessed 28 06 2024]