Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 165 (2022) 56205-56208

ISSN: 2229-712X

Active/Active failover using VPN

Khushbu Chauhan[1] and Sandeep Rana[2]

[1]Scholar in Computer Science, J.P. Institute of Engineering and Technology, Meerut.

[2]Department of Computer Science, J.P. Institute of Engineering and Technology, Meerut.

ARTICLE INFO

Article history:

Received: 22 March 2022;

Received in revised form:

22 April 2022;

Accepted: 30 April 2022;

Keywords

Routing,

VPN,

Tunnel,

Failover.

ABSTRACT

In any business network most important things that need to be addressed is up time. It depending on the size of the business and businessnetwork also, every minute downtime can more affect the productivity of the business employee andthe business system that use the network. The address this within the adaptive security appliance (ASA) product line, Cisco offers high availability through a series of failover capabilities. When configured, they allow a deployed ASA to be matedwith another ASA, which combine to offer little downtime if one of them encounters of failure [1]. This paper introduces the replication of data, it means both units carry data traffic and it also introduces how to secure our interesting traffic overthe internet. VPN mainly used for security purpose we use VPN in many thing and many fields. It provides the secure and private network connection through the public internet; the VPN protects our data in many ways. VPN tunnel is an encrypted connection between our device and VPN sever.

1. Introduction

It is a Cisco prosperity feature unique to the security appliance. Failover provides redundancy between paired appliances .The concept of ASA failover is simple in ASA failover two devices connected to the network and they connected to each other to communicate failover information traffic. One appliance backup another appliance. In active/active configuration failover happen only on a failover group basis not a system basis. If we appoint both failover group as an active on the primary unit, and failover group 1 fails, at that time failover remains active on the primary unit. While failover group 1 become on the secondary unit. Active/Active failover is only available on units that run in multiple context modes. Failover group 1 always a member of admin context. Failover group is a logical group of one or more contexts. In active/active failover we create a maximum two failover group. Tunnel mode protects the internal routing information by encryption the ip header of the original packets. It is widely implemented in the site to site VPN.

1.1 VPN (Virtual Private Network)

It provides security to our ip communication over the internet. The Internet Protocol Security is a secure and two-way means for connecting between private and public networks such as Wi-Fi networks and the internet. Encrypt all traffic by encryption using only licensed recipients, so that all traffic in transit may be unscrambled.

1.2 Tunnel

In the terms of computer networks tunneling is a communication protocol. It transfers the data from one network to another network in a secure way. Tunneling is a process in which VPN packets reach their destination, which is typically a private network.

1.2.1 Existing Work

The existing table show the how to create a active/active failover and how to make a failover link on ASA the configuration is given below.

1.3 Proposed Work

How does VPN tunnel work?

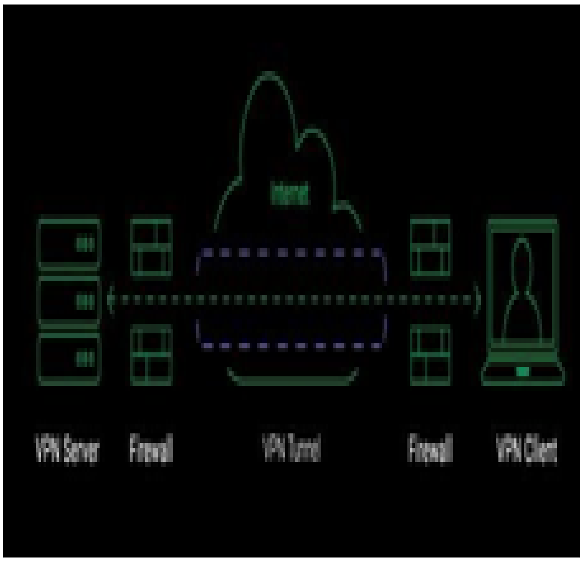

Figure.1 Working of VPN Tunnel

Here's how a tunnel work

- **Encryption the traffic-** when we use VPN the data protected from the third-party.
- **IP address hiding-** it provides security to our ip communication over the internet.
- **Wi-Fi hotspot security-** we don't need to be worrying our safety when we use public Wi-Fi.

Focus is to make an active/active using VPN we want to add security in this scenario. We have two sites in this topology we give VPN configuration on routers to provide security. Security association is a agreement between the 2 IPsec VPN.

Phase1 sa name- Isakmp Sa

Tele:
E-mail address: chauhankhushbu208@gmail.com

Phase2 sa name-Ipec Sa

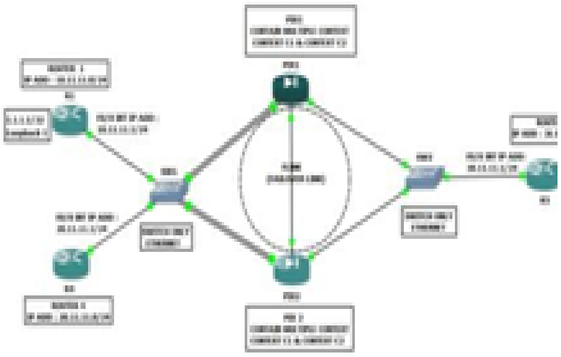

Figure 2. Active-Active Failover using VPN

Router 1: Configuration

```
#config t
#int f0/0
#ip address 10.11.11.1 255.255.255.0
#no shutdown #exit
#int loopback 1
#ip address 1.1.1.1 255.255.255.255
#no shutdown #exit
#ip route 0.0.0.0 0.0.0.0 10.11.11.10
#crypto isakmp policy 10 #Authentication pre-share
#Encryption 3des
#Group 2 #Hash md5 #Exit
#Crypto isakmp key Cisco address 30.11.11.1
#access-list permit ip host 1.1.1.1 host 2.2.2.2
#crypto ipsec transform-set tset esp-3des esp-md5-hmac
#crypto map smap 10 ipsec-isakmp #set peer 30.11.11.1
#set transform-set tset #match address 101 #exit
#int f0/0
#crypto map smap #exit
```

Router 2: Configuration

```
#config t
#int f0/0
#ip address 20.11.11.1 255.225.255.0
#no shutdown #exit
#ip route 0.0.0.0 0.0.0.0 20.11.11.10
#exit
```

ROUTE 3: CONFIGURATION

```
#config t #int f0/0
#ip address 30.11.11.1 255.255.255.0
#no shutdown #exit
#ip route 0.0.0.0 0.0.0.0 30.11.11.20
#ex
#Int loopback 1
#Ip address 2.2.2.2 255.255.255.255
#crypto isakmp policy 10 #encryption 3des
#hash md5 #authentication pre-share #group 2
#crypto isakmp key Cisco address 10.11.11.1
#access list 101permit ip host 2.2.2.2 host 1.1.1.1
#crypto ipsec transform-set tset esp-3des esp-md5-hmac
#crypto map smap 10 ipsec-isakmp #set peer 10.11.11.1
#set transform-set tset #match address 101
#exit #int f0/0
#crypto map smap
#exit
```

Asa Firewall Configuration When We Use Firewall Mid Of S2s VPN

To make here access-list for tunnel we have to give or open here three access-lists.

1: UDP 500

2: ESP

3: ICMP

```
#access-list out-in permit udp host any any eq 500
#access-list out-in permit esp host any any
#access-list out-in permit icmp any any
```

Conclusion

As we have gone through the possible details we conclude that VPN is the best opinion for the corporate networking. As many companies need to have access to internet and hence security is also the main concern. VPN provides best possible combination of security and private network capabilities with adequate cost- saving to the companies who are presently working with leased lines.

Table 1. ASA Failover Configuration

1	**Enter privilegedEXEC mode.**	**asa>enable**
2	Enter global configuration mode.	asa#configure terminal
3	Designate the ASA because the primary or secondary unit (default is secondary).	asa(config)#failover lan unit [primary | second ary]
4	Configure the ASA link which will be used because the failover link. Notes: The if name is employed to assign the name of the interface (don't use the name if command). The interface_id can bea physical interface, subinter face,or redundant interface; or an Ether Channel interface ID. On the ASA 5505, the interface_id specifies a VLAN ID.	asa(confi)#failover lan interface if_name interface_id
5	Configure the first and secondary IP addresses. Note: Both the first and secondary IP addresses must be within the same subnet.	asa(config)#failover interface ip if_name ip_address netmask standby ip_ad dress
6	Configure the ASA link that will be used because the stateful failover link. Notes: The if_name is employed to assign the name of the interface; this is often the identical because the failover link if name if they're being shared. The interface_id ma y be a physical interface, sub interface, or redundant interface; or an Ether Channel interface ID. On the ASA5505, the interface_id spec ifies a VLAN ID. This command is optional and is required on condition that stateful failover is being configured.	asa(config)#failover link if_name interface_id

7	Configure the first and secondary IP address for the state interface. Note: This step is required on condition that the link that's being used for the stateful failover link is different from the failover link. If it's being shared with the failover link, the data configured in Step 5 is used.	asa(config)#failover interface ip if_name ip_address net mask standby ip_addre ss
8	Configure the employment of IPsec on the LAN-to-LAN failover links (failover and stateful failover ,if configured). Notes: The key parameter will be up to 128 characters long This is the well-liked method to be wont to encrypt information over these links. OR	asa(config)#failover ipsec pre-shared- key key
8	Configure a failover key. Notes: The key parameter when usedwith the hex keyword is 32 characters. When it's used without it, it may be a string from 1 to 63 characters. This is a depreciated method of encrypting on these links, and it's not recommended in favour of the IPSec option above.	asa(config)#failover key {hex key | key}
9	Create a failover group. Notes: By default, group 1 is assigned to the first failover unit (as configured in Step 3). This command isemployed only configuring anactive/active failover.	asa(config)#failover group 2
10	Assign the group to a unit. Notes: Typically, group 1 is assigned to the first unit (the default), andgroup 2 is assigned to the secondary unit). This command is employed only configuring active/active failover.	asa(config-fover- group) # **primary** OR asa(config-fover- group) # **secondary**
11	Enter context configuration mode. Note: This command is employ only configuring active/active failover.	asa(config)#context name
12	Configure the context to be a member of a failover group. Notes: All unassigned contexts are assigned into failover group 1. The admin context is usually configured into failover group 1. This command is employed only if configuring active/active failover.	asa(config-ctx)#join- failover-group {1 | 2}
13	Enable the employment of failover on the ASA.	asa(config)#failover

1.2.2Behaviour of Active/Active Failover

Table 2. Failover Behaviour for Active/Active Failover

FailureEvent	**Policy**	**ActiveGroupAction**	**Standby GroupAction**	**Notes**
Aunit experiences a power or software failure	Failover	Become standby Mark as failed	Become active Markactiveas failed	When a unit ina failover pair fails, any active failover groups on that unit are marked as failed and become activeon the peer unit.
Interface failure on active failover group above threshold	Failover	Mark active group as failed	Become active	None.
Interface failure on standby failover group above threshold	No failover	No action	Mark standby group as failed	When the standby failover group is marked as failed, the active failover group does not attempt to fail over, even if the interface failure threshold is surpassed.
Formerly active failover group recovers	No failover	No action	No action	Unless configured with the preempt command, the failover groups remain active on their current unit.
Failover link failed at start-up	No failover	Become active	Become active	If the failover link is down at start up, both failover groups on both units become active.
Stateful Failover link failed	No failover	No action	No action	State information becomes out of date, and sessions are terminated if a failover occurs.
Failover link failed during operation	No failover	n/a	n/a	Each unit marks the failover interface as failed. You should restore the failover link as soon as possible because the
				unit cannot fail over to the standby unit while the failover link is down.

1.2.3 Active/Active Failover Feature Support

Table 3. Failover Features Support

Feature	**Active/ Active**	**Acti ve/Standby**
Single context mode	No	Yes
Multiple Context Mode	Yes	Yes

Reference

[1]https://www.pearsonitcertification.com/articles/article.aspx?p=2140095

[2]https://...networkgalaxy.org/2013/11/ci scoasaactiveactive-failover.html?m=1

[3]https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/ha_active_active.html

[4]https://www.cisco.com/c/en/us/suppor/doct/sec/asa-5500-x-series-next-generation-firewalls/110894-asa-active- active-failover-transparent.html

[5]https://cybernews.com/what-is- vpn/what-is-a-vpn-tunnel/

[6]https://www.google.com/search?q=TUNNEL+in+networking&oq=tunnel&aqs=chrome.1.69i57j69i59j0i271l3j69i60.3462j0j15&sourceid=chrome&ie=U TF-8

[7] https://www.nstec.com/what-is-vpn- router-alley/