Study of network security access technology based on VPN

Zhengrong Xiao[1, a], Yang Li[2,a] and Jie Li[2,a]

[1]China Unicom research institute, Beijing, China

[2]DIGITAL CHINA(CHINA)LIMITED, Beijing, China

[a]digital9898@sina.com

Keywords: VPN, LTE, IPSec

Abstract. Proposed a solution on existing mobile communication network system solutions and validated. Verification test of the gateway device construction show that IPSec gateway support IPSec functions, support IPSec VPN users access multiple functions; support IPSec different access VPN users can access different functions, support for AC and DC power supply mode, according to the site requires access to the appropriate power system.

Introduction

Data access via LTE to achieve VPN backup route for the international business, based on IP bearer network and 4G mobile networks, build a virtual private network for enterprises. This service is bundled with the VPN service. Users can uses IPSec, L2TP, RoutingBehind MS and other ways to achieve the fixed route backup protection to meet the needs of multi-branch interworking, the solution can also be applied to large domestic customers.

Terminal requirement

4G data access methods to realize VPN backup route service involved multiple networks, end to end service needs from the terminal, access network, core network, together with the bearer network, therefore, terminal is one of the important conditions to conduct business.

User-side access router is an access center of enterprise branch networks, the need to provide services for enterprise VPN access device, remotely access the corporate headquarters network to meet the requirements of the enterprise network information. To achieve VPN backup route business via 4G data access, requirements to terminal including the following aspects:

Functional Requirements in the user side:

- business functional requirements include router supports both fixed and mobile duplex mode of operation, when the network connection is working properly access way through the line, after a fixed routing failure, the wireless router can provide service as a backup route.
- access routers between the fixed and mobile operation mode automatically switches using protection mechanisms, the verdict mode can be designed by the companies themselves, to avoid false positives due to frequent switching.
- access routers should have the primary routing automatic recovery mechanism, when the primary link is restored connection, wireless router automatically cut off latency wireless router should be able to set up, in order to ensure that the primary route recovery process does not produce link outage.
- access router located in enterprise branch offices, should support the following features: (1)hanging multi-user; (2) may be linked to the user's IP address assignment via DHCP or a static setting; (3) When the switch occurs, the user's IP address will not change and can be done automatically through a wireless network access to corporate headquarters; (4) should support NAT.
- user side access routers should support local or remote access management, check the router connected device status, or some basic management operations.

- access routers support USB port to connect LTE data card can also be inserted into the USIM card directly through the manufacturer-specific 4G cards.
- long-running stability
- 4G network upgrade later versions support capabilities, such as from LTE to LTE-A evolution.

equipment needs of the user-side access router：

- Access Router as operator international customers access services ancillary products, elegant design requirements, the proportion of the coordination required to facilitate the placement, and recommended that the overall design of the gateway can simultaneously pay down, stand and hang three kinds of display mode.
- access router switch button should be simple and practical.
- access router must have sufficient indicator for simple indication of the operating state of the functional modules and networks.

Deploy of equipment

In IPSec solution, need to set up a access router at the user side supports IPSec protocol, enterprise network setting a IPSec gateway before PE router, to terminate the IPSec tunnel, and mapped to the appropriate VPN, complete the user's access. IPSec gateway device should have the following features:

- IPSec function
- support multi-access IPSec VPN function (ie multi-user shared IPSec gateway)
- support IPSec, different access VPN users can access different functions.

Direct Connect IPSec VPN ways to deploy wireless data access methods as a backup mechanism for VPN access business route.

In this deployment mode, IPSec routers and enterprise network access router equipment located inside the firewall, belonging to a private network connection, the user access to the VPN network through the packet domain core network equipment (which may be the core router, or a wireless network MME, can also be core routing switches, etc.),IPSec routers and CNCnet PE routers connected in parallel, its specific configuration as follows:

Connected to IPSec router via the mobile network packet domain core network equipment, and then through IPSec router and CNCnet PE router connected to complete the system interoperability, IPSec router and MME number of private network connections can be 1,2,3,4,. . . , N, can be a business use an IPSec router, it can be more of a public enterprise IPSec router with IPSec router connection CNCnet number of PE can be 1,2,3,4,. . . , N months, depending on the specific number of the actual situation in the provinces, each PE router and access router via IPSec packet domain core network devices are connected. In this way can make a considerable workload PE access router, but also an effective shared protection methods deployed in the above manner, the access of any one PE router fails, it can be assumed by other customers PE VPN access router device is connected to the bearer network.

Network deployment

In IPSec VPN mode, specific network deployment schematically shown in Figure 1:

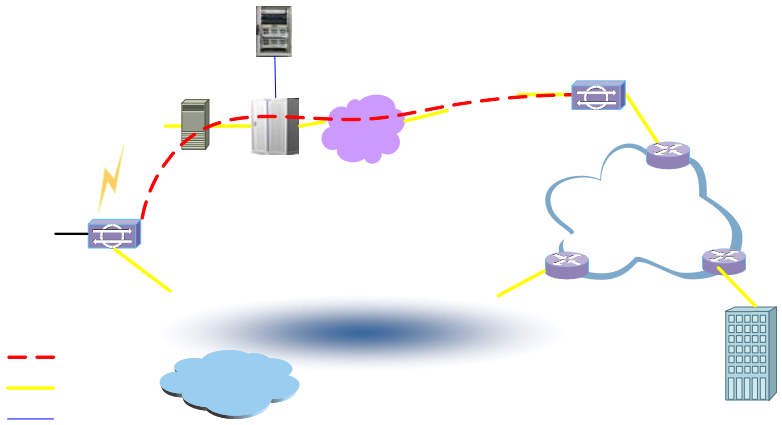

Figure 1. network architecture of IPSec VPN mode

Working mechanism deployed above is as follows:

First, the fixed broadband network support both fixed and mobile access router way to assign an IP address, Wi-Fi built-in USIM assigned a dedicated corporate APN for this router to routing parsing and IPSec tunnel establishment.

During normal operation, the access router wireless PDP does not activate the PS domain; declared along the route through the fixed network access router to PE1, by passing the VPN backbone network between this VPN PE PE1, so that users can access the enterprise through the line net.

When the fixed network failure, PE1 routing failures, first routing convergence, while the access router through a wireless network to activate a PDP context, the access router along the route declared through a wireless router to MME, and then the MME via the direct link routing information transmitted through IPSec router, declared by the IPSec router to PE2, by passing the VPN backbone network between this VPN PE PE2, until after routing convergence, users can access through a wireless PS domain enterprise network. Entire switching process switching time depends mainly on routes in the VPN backbone network convergence time, about a few seconds.

In this scheme MME functions for the existing network is not required, just the data can be transparently transmitted on the existing network MME devices without upgrading, IP address of wireless access router assigned by the MME.

Process of

In this mode, MME configure two address pools, one public address pool, and the other is a private network address pool. User card settled into the corporate card users and the ordinary user card, according to company policy, corporate card users are not allowed on the public network, so corporate users set specific user APN in the HSS, to distinguish it from ordinary user .

Processes are described as follows:

- after a fixed interrupt is detected by the access router, the flow is attached in the wireless side, the registered information on the MM context of the MME, HSS query to the user information.
- the access router uses queries to conduct business users dedicated APN PDP activation, MME according to the APN property, in a private address pool to assign an IP address to access the router, access router address assignment is enabled on the access router IPSec tunneling protocol to establish an IPSec tunnel on the route between the wireless router and the IPSec router until the end of this tunnel IPSec router.
- user access to the relevant company's VPN via IPSec router.
- route to the corporate headquarters of the enterprise network through backbone routers.

Test results

Through the existing network test, IPSec solution work well in the current network environment, complete the automatic switching between main and backup circuit to verify the feasibility of the scheme in the actual network conditions. test results are as follows:

（1）Link setup time test

Sigle user IPSec test				
	master—>backup (s)		backup—>master (s)	
	loss	delay	loss	delay
first	6	30	9	45
second	5	25	2	10
third	5	25	5	25

（2）service restore time test

Sigle user IPSec test				
master—> backup	Link setup time	Restore time	Wired link speed (Mbits/s)	Wireless link speed (Mbits/s)
	30s	60s	52	1.04
backup—> master	Link setup time	Restore time	Wired link speed (Mbits/s)	Wireless link speed (Mbits/s)
	45s	60s	52	1.04

Multiuser IPSec test				
master—> backup	Link setup time	Restore time	Wired link speed (Mbits/s)	Wireless link speed (Mbits/s)
	75s	88s	50	1.84
backup—> master	Link setup time	Restore time	Wired link speed (Mbits/s)	Wireless link speed (Mbits/s)
	19s	49s	50	2.4

In actual networking, if PE equipment Ethernet need to configure a static address, problems occur when switching, which is due to failure even if the fixed route, as long as there is no Ethernet port cable is unplugged, its port state is always for UP, PE does not think that this port failure, will not conduct a port routing convergence, while the access side has completed switching, routing, network access from another PE, corporate headquarters will find the same IP address has two routes, and could not determine that the route is broken. Links priority are not recommend , which will cause a lot of loss, the business can not be normal. Therefore, to ensure the normal switching operations, it is recommended that users do not use the Ethernet port to configure a static IP address.

Summary

Proposed a security access solution and validated. Through the verification test on the gateway device construction, IPSec gateway support IPSec functions, supports IPSec VPN users access multiple functions; supports IPSec different access VPN users can access different functions, support for AC and DC power supply mode, according to the site requires access to the appropriate power system.

Gateway device and 4G core network equipment is recommended MME placed in the same room, for easy post-maintenance management.

Acknowledgements

This work was financially supported by the project 2012AA01A403.

References

[1] Singh, A.K. ; Samaddar, S.G., Enhancing VPN security through security policy management, Recent Advances in Information Technology (RAIT), 2012 1st International Conference on, 2012 , Page(s): 137 - 142

[2] Weifeng Zhong ; Yanli Zhang, The design of VPN security gateway in remote monitoring system of rheometer, Strategic Technology (IFOST), 2011 6th International Forum on, 2011 , Page(s): 1109 - 1113

[3] Shihyon Park ; Matthews, B., Characterizing the Impacts of VPN Security Models on Streaming Video, Communication Networks and Services Research Conference (CNSR), 2010 Eighth Annual, 2010 , Page(s): 152 – 159

[4] Lakbabi, A. ; Orhanou, G., VPN IPSEC & SSL technology Security and management point of view, Next Generation Networks and Services (NGNS), 2012, Page(s): 202 - 208

[5] Uskov, A.V., Information Security of IPsec-based Mobile VPN: Authentication and Encryption Algorithms Performance , Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 2012 , Page(s): 1042 - 1048