Information and communication system technology with VPN site-to-site IPsec

W Sholihah, T Rizaldi and I Novianty

Computer Engineering, IPB Vocational School, Kumbangst. no. 14, Bogor, Indonesia

E-mail: walidah@apps.ipb.ac.id

Abstract. This research aims to solve network problems in Information and Communication Technology (ICT) project at Gelora Bung Karno (GBK) gym building. The ICT project was created for the 18th Asian Games event. The technologies used in ICT projects in GBK are VLAN (virtual lan) and Virtual Private Network (VPN). The problem in this ICT project is the end device must be connected through the two switched layers but using a different network. VLAN is a solution to divide the network segment without having to follow the physical condition of the device. This project was made by using four stages. Those stages are analysis, design, implementation and testing. On ICT systems, VLAN are used to divide network segments required for Access Point and CCTV requirements. VLAN are simulated in GNS3 and VMWARE software. As a result, access points and CCTV as end users are connected to the core routers in the network operational center via the layer two switch. The next problem is the lack of efficient monitoring and troubleshooting system. Monitoring and troubleshooting systems must be done from the Network Operational Center (NOC) in GBK. Monitoring and troubleshooting systems are more effectively done directly from the developer's local network by accessing the local network of ICT projects over the internet. This mechanism is called a VPN. VPN technology is used to access local networks that exist in ICT projects using the local network of related developer companies. The VPN uses IPSec as encryption for the packet data equality. The results show that VPN is able to connect local network in ICT GBK project with local network of developer company through internet.

Keywords—ICT, IPSec, VLAN, VPN

1. Introduction

The Information and Communication Technology (ICT) project at the Gelora Bung Karno gym building (GBK) is being prepared for the 18th Asian Games. The purpose of this ICT project is to build a free internet connection system throughout GBK building; an Internet connection using wireless system. This ICT system requires 124 access points scattered throughout the GBK area. In addition, the ICT project also built a security system using CCTV. Access Point and CCTV positions can be seen in Figure 1. The VLAN is connected to the Network Operational Center (NOC) for monitoring all devices. The vendor used on this project is Cisco.

VLAN (Virtual LAN) is a technology that allows a LAN (Local Area Network) is divided into several different networks. VLAN can divide the network virtually without having to follow the physical condition of the device. VLAN can also improve network performance because each broadcast only sends the domain of the network itself. According to [1], a VLAN is a logical group of network users and resources connected administratively defined ports on a switch. In [2], a VLAN is a...
set of workstations within a LAN that can communicate with each other as though they were on a single, isolated LAN. In [3], VLAN technology is used to segment a complex network into smaller networks for better manageability, improved performance and security. VLAN logically creates segments within the switch based on an organization’s function such as department or geographical locations. This minimizes the use of resource switches when sending broadcasts. In addition VLAN can also minimize the use of costs in terms of procurement tools and network infrastructure needs, simplify management, and improve security.

Figure 1. ICT project map in GBK.

Network monitoring and troubleshooting system in GBK is done by developer. The distance between the project site and the developer's office becomes an obstacle. The problem is that there is an efficient mechanism that can connect the local network in each project with the local network in the developer's office. This can be solved by using VPN. VPN can connect both local networks through internet connection. VPN utilizes a public network (e.g. Internet) to build up a network only for private use [4].

This form of network requires a good security system so that the local network can not be accessed by unauthorized users. Internet Protocol Security (IPSec) builds a good encryption system as a security system. IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host) [5]. IPSec is a set of security protocols which was developed by IETF (Internet Engineering Task Force) in November of 1998[6]. IPSec is a set of protocols operating at the OSI architecture model Network Layer by extending the IP packet header to support secure exchange of packets [7]. IPSec offer data integrity, data confidentiality, and authentication originality of data at the network layer in OSI model [8]. IPSec provides a secure tunnel between two devices such as two directly connected routers. IPSec determines which packets should be sent through this tunnel. IPSec also specifies what parameters should be used to protect packets sent through tunnels to peers over long distances. VPN with IPSec is network monitoring solution to enterprise business improvement in virtual enterprise network [9].

2. Method
The method used in this study consists of four stages. The first stage is problem analysis. The problems encountered are the interconnection of device access point and CCTV that must be
connected to the NOC through a two layer switch (using a VLAN system.) Next, monitoring and troubleshooting local networks that exist in the ICT GBK project using the IPSec VPN.

The second stage is designing. At this stage a network topology is used to solve both problems. The equipment used is cisco router c7200 image, layer switch three cisco image, switch layer two cisco image and client vpcs. All images are simulated using GNS3 and VMWARE applications. GNS3 is used for creating the topology to create the network involving two tunnel end points in order to make a secure connection for secure transmission of data [10].

After the stage of analysis and design is completed then go into the implementation stage. This stage of implementation is a step for the configuration of the tools used. Configurations that made are IP configuration, VLAN interface configuration, routing configuration and lastly NAT configuration.

The last stage is testing. At this stage an interconnection test is performed between VLANs and VPN tunnel implementations that connect the local network of ICT projects with the local network of developer offices.

3. Results

This research is done by simulation on GNS3 application by using the appropriate device. Because there are limitations on virtualization, access points and CCTV are replaced by VLAN access client by using client vpcs. The network topology implemented in this project can be seen in Figure 2.

![Figure 2. Network topology of ICT project.](image)

In Figure 2, layer two switched, layer three switched and routers are cisco products. Client vpcs in Figure 2 as device access point and CCTV. Access points and CCTVs are connected with layer two switched using a VLAN system. Access points using VLAN id 8 which uses port ethernet1/0-3. CCTV uses VLAN id 130 which uses ethernet2/0-3 interface port. In the ICT project, the cables used to connect access points and CCTV to layer two switched are fiber optic cables with 1Gb/s speed. The layers two switched are connected to the layer three switched in NOC. The ethernet0/0 port on the second layer switch is connected to the layer three switched. Because this port will bypass the various VLANs, then this port is configured as trunk port. The cable used to uplink from layer two switched to layer three switched using fiber optic which speeds up to 10 Gb/s. The layer three switched, for DHCP server, serves to dynamically distribute IPs to VLAN interfaces id 8 and 130. Additionally, the layer
three switches also serve for routing to the router. This routing serves to send packets from the layer three switch to the Senayan router. The layer two switches are connected to the layer three switch using fiber optic at 10 Gb/s. Uplink from layer three switch to router also use fiber optic with speed 10 Gb/s. The interface ports used from the layer three switch to the router with fast ethernet 0/0 interface and the router's fast ethernet interface 1/0. Router is used to connect private networks that exist in ICT projects with internet. The mechanism used is NAT and routing.

In Figure 2, the right side represents the internal network of the developer office and the left of the local network of ICT GBK project. Both local network systems are connected to the Internet. At this stage a VPN tunnel is formed with an IPSec security system. The yellow line (box with dashed lines) represents the tunnel VPN path that is formed to interconnect the local network between the GBK project and the developer's office. The Internet is an ordinary router that manipulated as a public IP with dns google from IP loopback 8.8.8.8/32.

![Figure 3. DHCP VLAN testing.](image)

![Figure 4. Failed test example.](image)

Figure 3 and Figure 4 are VLAN testing. This test is performed on the vpcs client (as access point and CCTV). Both have been assigned VLANs id 8 and 130 which means it will get IP 192.168.8.6/24 and 192.168.130.6/24 according to the DHCP pool specified on the DHCP server layer three switch. Each client gets an IP as defined in the DHCP pool and obtains an IP range outside of IP that should not be distributed (1 until 5).

This vpcs client uses the command line interface. So to request the IP of the DHCP, the server is using command “dhcpp”. DDORA is the four stages passed until the client gets IP (GAmbar 3). The first D, DHCP is running service. The second D is discover. Client will broadcast to search for available DHCP server. Once it's found, the DHCP server offers IP leasing to the vpcs client. This step is called the offer. The client vpcs will then ask the server to rent out the IPv4 address listed in the request message. The last step is acknowledgment. The DHCP server specifies the IP address, network, and default router. That four steps are process to request IP lease from DHCP server. It means DHCP service is running well. Client vpcs gets IP 192.168.8.6/24 with gateway 192.168.8.1 (access point) gateway and IP 192.168.130.6/24 with gateway 192.168.130.1 (CCTV). Network id 8 and 130 are in accordance with the VLAN id that has been configured which means VLAN access has also been successfully implemented. Figure 4 is an example of a DHCP service failure. The message DDD means the client continues to broadcast to search for DHCP server but still not found and finally “can not find dhcp server”.

Figure 5 and Figure 6 show the ping test from the VLAN client to the internet using loopback IP manipulation 8.8.8.8 as the internet in the cloud. The router will translate the local network 192.168.8.0/24 and 192.168.130.0/24 to access the internet through the fastethernet0 / 0 output interface on the router that connects directly to the cloud internet.

In Figures 5 and 6 each client already has an IP of the DHCP service whose network id is matched to a configured VLAN id. Figure 5 shows the client access point gets IP 192.168.8.6/24 with gateway...
192.168.8.1. The command to see this IP is "ship". The same is done in CCTV client in Figure 6. Client gets IP 192.168.130.6/24 with gateway 192.68.130.1. This client must be connected to the internet. Testing is done by ping command 8.8.8.8 (IP 8.8.8.8 is in the cloud internet).

Seen in Figures 14 and 15 the result of ping 8.8.8.8 outgoing messages of 84 bytes from 8.8.8.8 icmp_sq = 1 ttl = 253 time = 61,508ms means the packet has reached the internet and returned to the client with icmp protocol. If the failed message that came out of ping 8.8.8.8 is request time out or destination unreachable. This means that packets are not sent to the internet. This test has been successfully done because the client can access Internet cloud with IP 8.8.8.8 from local network with network 192.168.8.0/24 and 192.168.130.0/24.

The first test phase on the VPN is to test the connection by using the ping command in the command prompt on the windows client that is in the local network of the developer's office. The windows client uses the 192.168.3.2/30 IP address with the 192.168.3.1/30 gateway. Client will send ping packet to ICT GBK project that is 192.168.1.1/30.

In Figure 7 the output of the connectivity test results with the ping mechanism is successful. Client windows that have IP 192.168.3.2/30 residing in the private network of developer office can ping the IP 192.168.1.1/30 which is in the local network ICT project GBK. Reply from 192.168.1.1 means the packet from the IP network 192.168.1.1 is accepted in the windows client with IP 192.168.3.2. Thus the windows client located on the local network of developer companies are already connected to the local network that is in the ICT project GBK.
Figure 8 is the result of tracing route testing using tracert command on windows client. In this test which the package from beginning to end, through was the path. The VPN tunnel feature makes the path through which a path has been created. Basically the packet passes through public IP connections. Client windows that perform tracing route or route traveled through the package from the local network to the gateway located in the router office developer with IP 192.168.3.1. The packet goes directly through VPN tunnel. It is marked by connecting it to the gateway in the ICT project router as shown in Figure 8. The packet that has already passed through the gateway with IP 192.168.3.1 goes directly to the router in the ICT project on IP 192.168.1.1. It is shown in Figure 8 in the form of a text message "tracing route to 192.168.1.1 over a maximum of 30 hops", it means that the maximum packet path is skipped ie 30 IP jumps. Because the VPN tunnel is created directly to the router so there are only two jumps or hops traversed as in Figure 8, 51ms 9ms 9ms 192.168.3.1 and 2 103ms 72ms 92ms 192.168.1.1.

4. Conclusion
ICT systems created to provide wireless internet connection for Asian Games visitors in the area of GBK and increased security with the CCTV. Access points and CCTV are organized with VLAN that allow virtual network sharing. This can reduce costs. The VPN tunnel system is also built to facilitate local network access of ICT projects from developer offices via the internet to monitor and maintain the existing devices in ICT projects.

References
[1] Pal GP and Pal S 2013 Virtual Local Area Network Int. J. Sci. Res. Eng. Technol.1(10)006-010
[2] Tambe S S 2015 Understanding Virtual Local Area Networks Int. J. Eng. Trends and Technol. 25(4) 174–176
[3] Shaffi A S and Al-obaidy M 2012 Effective Implementation of VLAN and ACL in Local Area Network Int. J. Inf. Technol. Bus. Manag.4(1) 46–52
[4] Wang X andPeng X 2015 VPN Gateway Research in Wireless Network Based on SSL Technology Int. J. Sci. Technol.8(4) 17–26
[5] Singh A andGahlawat M 2012 Internet Protocol Security (IPsec) Int. J. Comput. Networks Wirel. Commun. 2(6) 717–721
[6] Chawla B K, Gupta O P andSawhney B K 2014 A Review on IPsec and SSL VPN Int. J. Sci. Eng. Res. 5(11) 21–24
[7] Alshamrani H 2014 Internet Protocol Security (IPsec) Mechanisms Int. J. Sci. Eng. Res. 5(5) 85–87
[8] Ahamed R and Rajamohan P 2011 Comprehensive Performance Analysis and Special Issues of Virtual Private Network Strategies in the Computer Communication: A Novel Study Int. J. Eng. Sci. Technol. 3(7) 6040–6048
[9] Rosu S M, Popescu M M, Dragoi G and Guica I R 2012 The Virtual Enterprise Network based on IPsec VPN Solutions and Management Int. J. Adv. Comput. Sci. Appl. 3(11) 26–34
[10] Sharma T andShiwani S 2013 Statistical Results of IPsec in IPv6 Networks Int. J. Comput. Appl. 79(2) 14-19