Interested in learning more about security?

SANS Institute InfoSec Reading Room

Network Based VPNs

Over the past few years, the Virtual Private Network market has drastically evolved. VPNs grew and became more complex because of various supplementary functionalities. In addition to these technical issues, ISPs saw in VPNs an opportunity for business and increased profitability. They searched for a large-scale solution that would allow them to propose hundreds of large VPNs with multitude of added features and that would be easy to manage and maintain. The result was the emergence of a new type of VPN, Network based ...

Network Based VPNs

Practical: Track 1- GIAC Security Essentials (GSEC)
GSEC Practical Requirements (v.1.4b) (August 2002), Option 1
Author: Olivier Strahler

Table of Content

1. Abstract

Over the past few years, the Virtual Private Network market has drastically evolved. VPNs grew and became more complex because of various supplementary functionalities. In addition to these technical issues, ISPs saw in VPNs an opportunity for business and increased profitability. They searched for a large-scale solution that would allow them to propose hundreds of large VPNs with multitude of added features and that would be easy to manage and maintain. The result was the emergence of a new type of VPN, Network based VPNs.

This paper focuses on this particular type of VPN. First, it provides a short history on the evolution of VPNs, then it explains what is meant by Network based VPNs. To best present this concept, I will use a standard company network for which a CPE and a Network Based Solution is proposed and I will compare the 2 alternatives. Such an approach will allow identifying the differences in design and addressing some fundamental pre-requisites for the implementation of Network Based VPNs. I will review some important security issues to address when an ISP deploys such IP Service Switches. To finish up, we will be giving a list of the major PROs and CONs of Network Based VPNs.

2. History of VPNs[1]

Rapid development of Internet over the past few years and its use as communications means for critical business data has led to the emergence of Virtual Private Networks.

The first generation of VPNs is based on hardened systems running VPN software.

The second generation of Virtual Private Networks was well known FW vendors that have integrated VPN software. They provide the functionality but they do not yet allow good VPN performance (e.g. 3DES encryption) as the hardware is specifically built for FW tasks, thus packet inspection.

The third generation of VPNs is based on dedicated hardware often referred to as "VPN appliances". These devices have dedicated hardware to accelerate encryption. Very often, they also include a more or less robust Firewall and other functionalities such as QoS, VoIP, etc.

With the evolution of today's business practices where home workers are common practice, fast and reliable communication between branch offices around the world and

[1] Cosine Communications. URL:http://www.adimpleo.com/library/cosine/cosinewp.pdf

the headquarters become critical and most importantly, where costs are a determining factor for business survival, a multitude of VPN solutions have evolved[2].

The best known and most commonly used VPNs today are "CPE based ones".

CPE Based VPNs:
In Customer Premises Based VPNs, as the name implies, the devices that are involved to set up the VPN are located on the customer's facilities.

The issues with CPE based VPNs are that they represent an important capital expenditure because they require a lot of equipment. Also, they are not very scalable because of the increased complexity in managing them. CPE based solutions could be implemented and maintained by the company or could be outsourced to an ISP or third party Integrator/Consultancy Company.

Because of important "capital expenditure" for CPE based VPNs and the scalability issues, especially for Service Providers that maintain multiple VPNs, a new type of VPN has emerged, Network Based VPNs[3]. As opposed to CPE based VPNs, where each site participating in the VPN needs to have its own VPN device and FW, in a Network Based Solution the intelligence of the VPN is moved to the edge of the Service Provider Network. This requires very powerful "Carrier Class" equipment.

During the last year, there has been a rapid growth of hybrid solutions[4]. Basically, hybrid solutions are Network based VPNs using high-end CPE based VPN equipment. The reason for hybrid solutions is to take advantage of the scalability and the decreased costs while keeping implementation and Management Control in-house.

3. Network Based VPNs

3.1. Definition

The main characteristic of a Network based VPN is that all the devices involved in building the VPN are shared systems owned by the ISP and located at the edge of the ISP's backbone. Those shared devices run several different virtual instances which are then assigned to one or multiple customers. This means that multiple VPNs each from a

[2] Tim, Greene. URL: http://www.nwfusion.com/newsletters/vpn/2002/01674562.html
[3] David, Willis. URL: http://www.nwc.com/1316/1316colwillis.html
[4] Bryan, Meckley. URL:
http://www.oft.state.ny.us/security/electronic%20presentations/conference2001/CPEvsNET_VPN.rtf

different company run on the same device. Those Carrier-Class VPN devices are also very often referred to as IP Service Switches.[5]

> **Network Based VPNs:**
> *"Network based IP VPNs, can be efficiently delivered from the service provider's network edge, or point of presence (POP), to a customer's premises over a no- frills WAN link. No CPE is required except for a standard IP router. This allows the service provider to house all VPN functionality in their network without setting up and managing expensive onsite CPE."* [6]

The biggest consequence for a company when deciding to implement Network based VPNs is that, by definition, it implies the outsourcing of both your VPN and your FW solution. This assumes a detailed and precise developed security policy as well as concise procedures prior to implementing such a solution

3.2. Outsourcing

In the cases of outsourcing security related tasks such as VPNs and FWs, companies need to carefully assess the risk and implications of their decision.

The main reason for outsourcing is the lack of in-house resources as well as cost concerns. While outsourcing, an important aspect to consider is the structure of a company's security policy and its compliance with outsourcing its VPN and FW solutions. Companies are often mistakenly thinking that outsourcers are responsible for defining their security policy. Such an approach is not only unwise but also very risky.

Outsourcers do neither know the specificities of each particular client they work with, neither the part of the organization's infrastructure that is critical nor the data that is valuable and should be kept confidential. The company could require the Outsourcers to comply with its security policy when implementing a solution, most of the time however, this is not very practical. A good approach would be to translate the security policy into appropriate NDA agreements and SLA's that reflect the company's needs. For example, if a company is in the e-business, the availability of its web-servers is a critical factor to them and therefore it requires its Outsourcers to provide 100% availability for its Web Servers and the connected databases. Therefore one of the Service Level Agreements should state: Web-Service and Database availability = 100% and a precise list of Web-Servers and Databases should be included.

Thus, it is clear and logical that before the final decision to outsource, all the companies should not only define their security policy based on their business and their

[5] David, Holdes. URL: http://www.broadbandpub.com/broadbandworld/v3n2/survey2.pdf
[6] Corona Networks. "Delivering Next Generation IP VPN Services". February 2002
URL:http://www.coronanetworks.com/products/whitepap/documents/NextgenIPVPN.pdf (Jan 15 2003)

company culture but also validate that the outsourcer's standard procedures for implementing and managing their VPN and FW are compliant, or could be easily adapted to the particular needs of their security policy. Obvious examples of this are Change management procedures (who can change FW rules, which authorization is required), remote access (does your policy allow remote access to 3rd Parties for maintenance), etc…

After taking into consideration some essential aspects when outsourcing, the next step is to look at Network Based VPNs structure, the means to secure them and some practical tips to consider.

4. Security & Design

The easiest way to show what a Network based VPN looks like is to make a diagram of the well known standard (CPE based) VPN solution and then redraw the same VPN in a Network Based Scenario. Let's consider a standard network with a few branch offices connected to a central site, the headquarters. The headquarters also have a DMZ for their Web Servers, Mail Servers and external DNS. Of course the company has foreseen Remote Access for its mobile employees.

4.1. CPE Based Solution

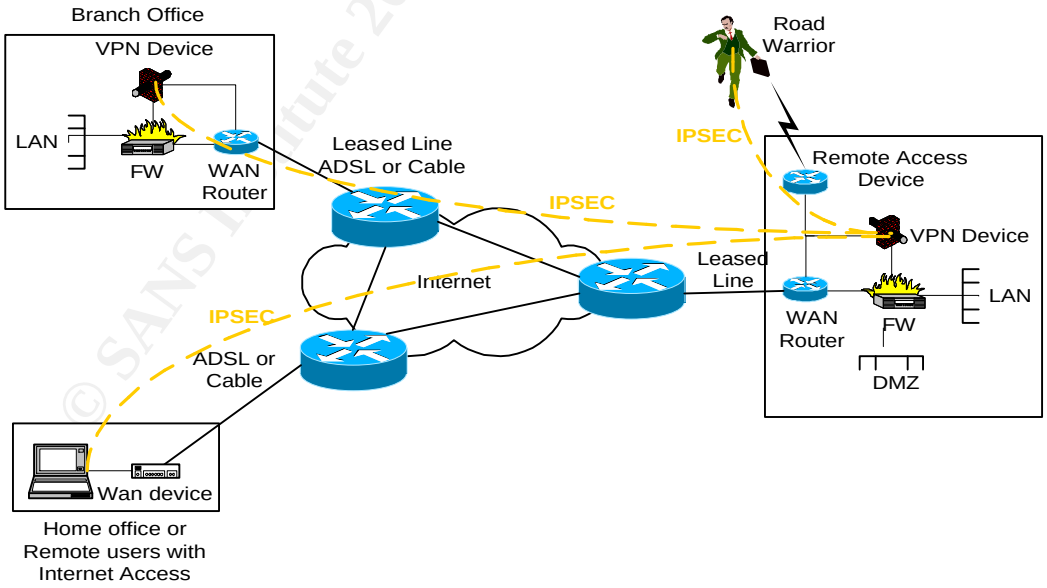

Figure 1: Classic Customer Premises Based VPN

Figure 1 shows a standard Customer Premises Based Firewall that includes the most common features already mentioned above. Let's review this diagram with more details.

Depending on the size of the branch office (or more precisely, the amount of traffic generated by the branch office), it can be connected over a dedicated (leased) line or with a DSL or Cable connection. Besides the POP router, the WAN device (Router or Cable modem, depending on the connection) is attached to two devices. The first device is the VPN device which terminates the VPN tunnel through which all internal traffic passes, the VPN device is in turn connected to the FW. The second connected device is the FW which protects the Internal Network and controls all incoming and outgoing traffic. The firewall sends traffic destined for the Internet unencrypted to the ISP. The traffic destined for the remote Private networks is sent to the VPN device for encryption before it is sent over the Internet to the Remote VPN device.

For Remote users, the "VPN device" is replaced by a software module running on their PC. This is valid for Home users with an internet access as well as for users that need a corporate dial-in. The reason for this is very simple. Experience has shown that users are often confused and they never remember when the usage of their VPN client software is necessary and when not. In the diagram above, the VPN client is always required, no matter what the underlying connection is. Although not really necessary when dialing into the corporate RAS Server, activating the VPN makes the usage of the remote access simpler for both the users and even for the administrators. The use of the VPN client software while in dial up allows employing one authentication mechanism for all "remote access" scenarios. In addition it enables the possibility to use a third party dial-up services such as I-Pass or free Dial-up. At the same time, it provides a very good protection against war dialing, if a hacker manages to successfully dial into the RAS server by exploiting vulnerability in the RAS authentication, he would still require authenticating to the VPN device in order to get access to the corporate LAN. (Principle of defense in death)

The central site (generally the headquarters) is the endpoint of all the VPN tunnels. Besides the VPN device (which is generally a more powerful version of the VPN devices installed in the branch offices because it terminates all the tunnels), the central site generally also hosts the RAS Server for dial up as well as all the Internet Facing servers such as Mail, Web, external DNS, etc… To be able to do so, the central site should have three Zones. The first Zone is the local LAN, the second zone is the DMZ (demilitarize Zone) holding all the internet facing servers and the third Zone hosts the VPN Devices and the Remote Access Server.

4.2. Network Based Solution

Transforming the above VPN diagram into a Network Based VPN gives a new structure as presented here under.

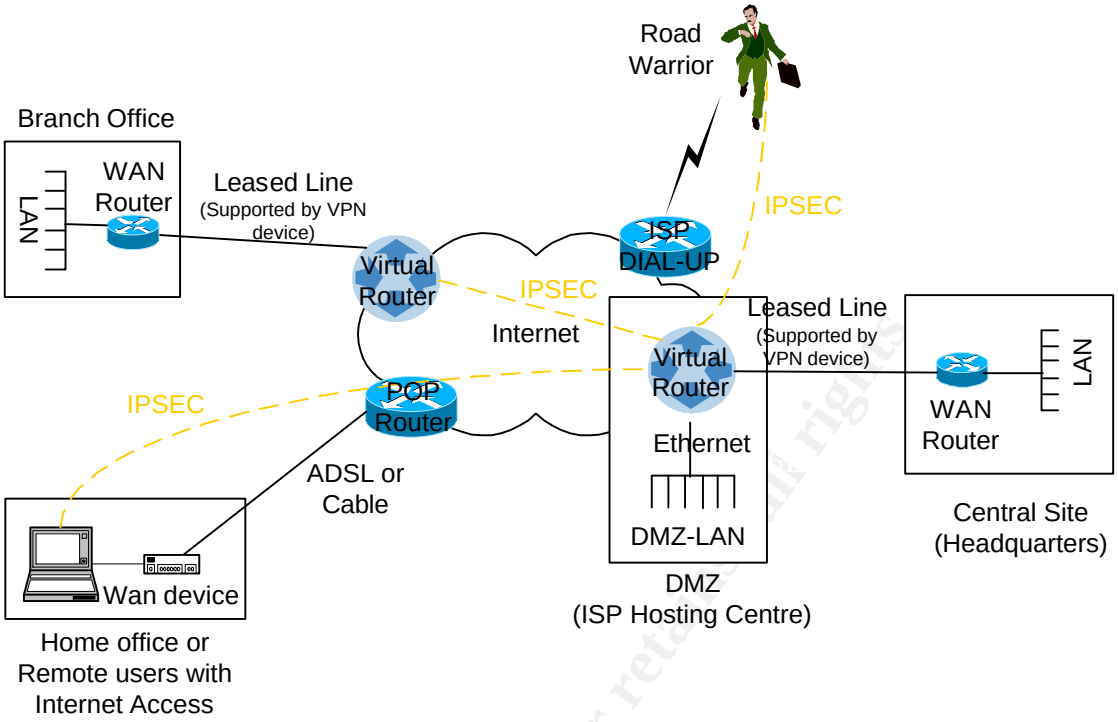

Figure 2: Classical Network Based VPN

The structure of the Network based VPN is very different from that of the CPE based VPN. Although the VPN offers nearly the same functionalities as the previous solution (except that there is no corporate dial-up server), the way it is structured and the places where the traffic is encrypted are substantially different.

As mentioned earlier, all the intelligence is on the Carrier-Class devices sitting on the ISP's network edge and run the Virtual Routers. The name "Virtual Router" is misleading; in fact besides the Virtual Routers, other virtual instances deliver much more functionality than pure routing. They provide a multitude of services such as Firewalls (Packet Filter, SPF and Proxy), VPN encryption, anti-virus, etc…. The functionalities vary slightly from one vendor to another.

As shown on the diagram, IPSEC tunnels are created between the Virtual Routers and traffic on the Local Access[7] is unencrypted. This design is of a great importance because; in order to guarantee confidentiality the traffic on the Local Access needs to remain on a dedicated private data-link. The Local Access needs to be a dedicated Point-to-Point connection between the Customer's premises up to the Virtual Router. Therefore, it is impossible to use shared circuit aggregation equipment to terminate the Local Access on the POP side.

[7] Telecom line between Customer Premises and the ISP's Point of Presence (POP)

This implies that when a Network Based Solution is implemented, the company is limited to the telecom technologies supported by the VPN hardware used by your ISP. Most of the time those Carrier-Class equipments are very modular and the limitation is very often the ISP's choice of which Local Access to support.

To illustrate the above, please review the figures below.

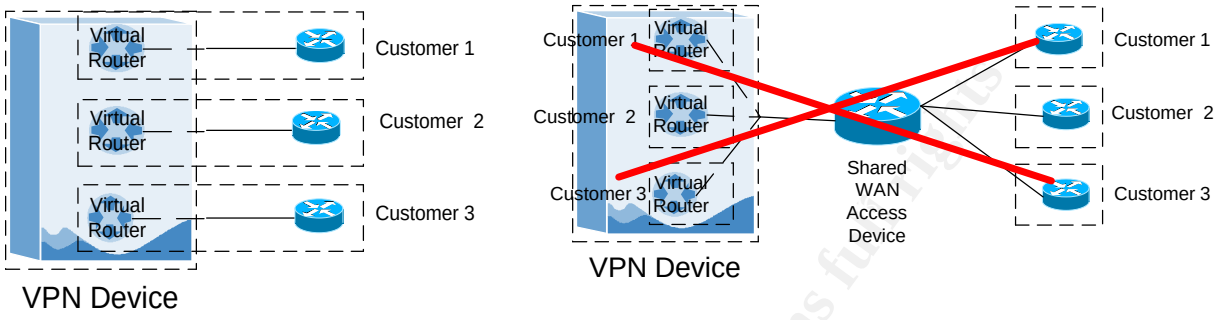

Figure 3: Correct versus Incorrect method of aggregating Local Access

Another important aspect that comes out of the above is that when a VPN is built, the connected site needs to be in the reach of the ISP providing the VPN. For example, if there is a remote office in Nairobi (Kenya) but the closest POP where the ISP has one of his VPN Devices is in Rabat (Morocco) then the purchase of a dedicated line all the way from Nairobi to Rabat (where one can plug into the VPN device and connect to a Virtual Router) is necessary. The need for dedicated lines also excludes all types of shared media access such as Cable Technology as connections to the VPN.

For these "Offnet" sites, the best solution is connecting the site to a local ISP and using a VPN device on the Customer Premises Site that builds an IPSEC tunnel to one of the Virtual Routers. Such an answer to the problem is equivalent to the Branch Office in the CPE based solution illustrated in Figure 1: Classic Customer Premises Based VPN except that the tunnel endpoint is a Virtual Router instead of another VPN device.

The same solution is available for Home users with a permanent internet access except that the VPN device that builds up a VPN tunnel to the Virtual Router is in fact a software running on their PCs. Mobile users employ the same solution; however, since the central site does not have any specialized equipment in its premises, it does not provide RAS servers for the mobile users to dial in. It is therefore necessary to foresee some dial-up access. An example of a global dial-up solution is I-Pass from Infonet but others, such as MSN, AOL, etc… provide similar services.

This brings up IPSEC compatibility. IPSEC is the protocol used to build the encrypted "tunnels" that link the different sites participating in a VPN. IPSEC is a fairly new protocol and the definition of its standards is not yet finalized. References on IPSEC and milestones of the IPSEC workgroup of the IETF can be found at: http://www.ietf.org/html.charters/ipsec-charter.html. Most Network-Based VPN vendors,

however, have tested multiple equipments from their direct or indirect competitors and provide a compatibility list as well as (if applicable) special configurations required to build IPSEC tunnels between their own and their competitors' devices. This is also valid for VPN software used on PCs for building tunnels to the virtual routers.

The biggest difference between Network Based VPNs and CPE based VPNs is at the Headquarter site. In fact Network-based VPNs do not allow DMZ's located at the customer premises. As usual, there is a workaround which consists of treating the DMZ as a separate site and installing it using a separate VR and a separate local access. I will not develop this alternative here as this is one of the simpler solutions used only on rare occasions because it requires an additional costly leased line. In a network based VPN, the best alternative for DMZs is to use collocation services from the ISP and connect the DMZ through Ethernet to the Virtual Router. Hosting services are another aspect to verify against the security policy before doing it. The most significant implication when collocating servers to foresee is 24/7 "remote hands" support provided by the collocation partner as well as remote access for management. In most cases, Remote Access to Internet facing servers is installed even when located in-house. Generally, the servers allow SSH connections from specific IP addresses on the corporate network. An alternative way to provide remote management or a backup solution for server management is to install a terminal server that connects to the console ports of the various servers. The terminal server could be accessible over a secure modem such as IRE or Mykotronx PALLADIUM[8].

4.3. Virtual Router

Virtual Router:
"A Virtual Router (VR) is an emulation of a physical router at the software and hardware levels"[9]

While I have reviewed the Network Based VPN scenario, I have often spoken about Virtual Routers. As mentioned earlier, the name "Virtual Router" is misleading; in fact besides the Virtual routers, other virtual instances deliver much more functionalities than pure routing. Various types of virtual instance are available. To cite just a few examples, you can run virtual Firewalls, virtual anti-virus, virtual VPN encryption, etc… The functionalities slightly vary from one vendor to another.[10] In fact, most vendors provide APIs which allow third parties to develop applications that run as virtual devices. For example, when considering the Cosine IPSX 9500 VPN platform, one well known application that has been adapted to work on their switches is for example is the Checkpoint FW[11].

[8] Product Description, URL: http://www.pc-card.com/product.cfm?productid=884
[9] Jessica, Yu. URL:http://www.nanog.org/mtg-0102/ppt/yu.ppt
[10] Curt, Newton. URL: http://www.nwfusion.com/news/tech/2001/0416tech.html
[11] Cosine Communications. URL: http://www.cosinecom.com/newsevents/pressreleases/20010605.html

Developing all the functionalities of those virtual devices goes beyond the scope of this document. However, for the curious reader who wants to get a good understanding of virtual routers I suggest the White Paper from Futuresoft. [12]

5. Management & Reporting

Another important aspect of the network based VPNs is their administrative side and most of all, the security concerns such as the management Network that is very often overlooked. For example, the case in which a hacker gains access to the management of the IP Service Switches on which an ISP's customers are running, would compromise all the VPNs. Not only would the confidentiality of all the ISP's managed VPNs be compromised but the hacker could simply delete the configuration of the switches which would take down all VPNs configured on or transiting through the affected device. A more malicious hacker however, would not do such an obvious thing. Instead, when he has finished collecting confidential information from the VPNs he gained access to, he would simply reconfigure the Firewall instances running on the compromised IP Service Switches to run different types of proxies without logging that he could then use in the future to daisy-chain his IP connections in order to make it difficult to be tracked. Therefore, when an ISP deploys such type of devices, a private network allowing secure management of such devices, should be foreseen. This private network should be totally isolated

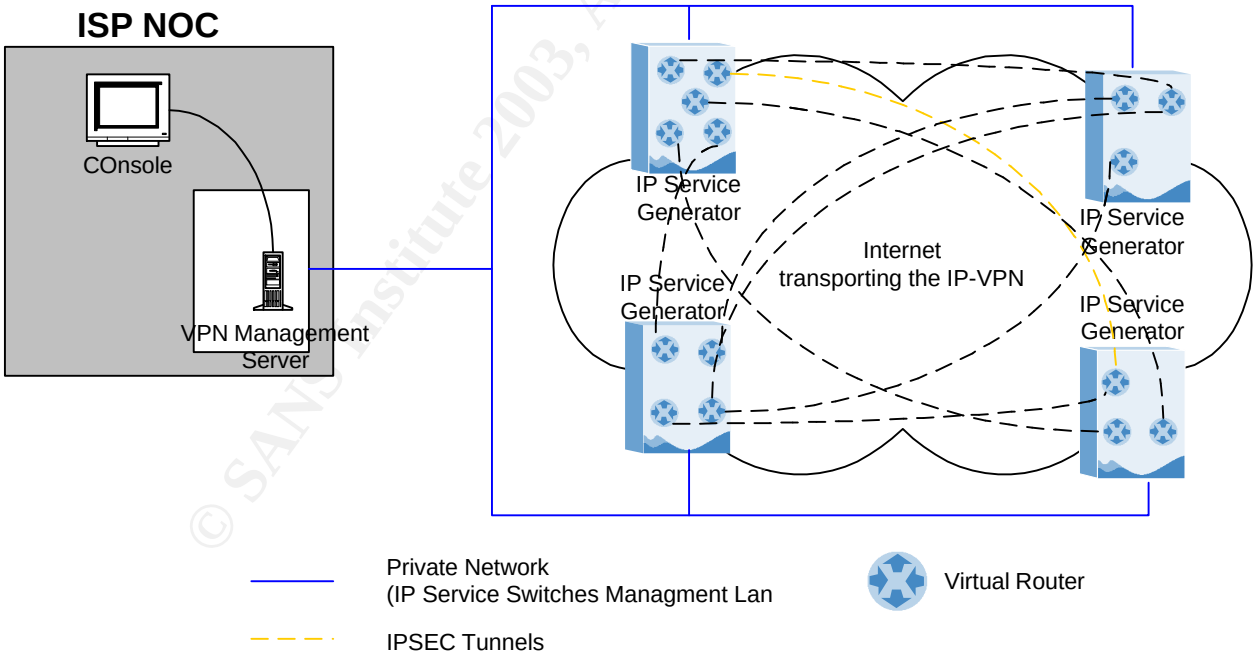

Figure 4: IP VPN Device Management

[12] Futuresoft. URL: http://www.futsoft.com/pdf/Virtroutwp.pdf

Even though the above solution seems to be not only simple but also secure, there are additional factors such as the two listed below that complicate and weaken it.

1. Management possibility for the VPN customer
2. Real time Performance and Security Reporting

Although most of the VPN management is done by the ISP, some VPN customers like to keep some control over the VPN, especially certain daily tasks such as adding and deleting Remote VPN users, modifying FW rules to allow access to additional web servers, etc... To do so, the ISP needs to provide its customers with an interface through which they can perform such changes. This interface must be able to write to the Management Server which in turn configures the VPN Devices. The biggest issue when providing access to equipment shared amongst multiple customers is security, especially when access is given over unsecured channels such as for example the Internet. Most, if not all vendors, provide Management software that allows configuring and maintaining all aspects of the VPN (Virtual Router, Firewall, IPSec tunnels, Remote Access Users, etc…).[13]

The second aspect that needs to be taken into account is reporting. Most, if not all VPN customers require reporting on the performance of their VPN as well as their Security Incidents. Therefore, the ISP needs to foresee a way of collecting data.

Most of the Vendors permit to collect data (Syslog and SNMP Traps) from the Switches through the management Network. For the majority of switches, since the information is collected over the management LAN, the logs or the SNMP traps contain data from the complete switch, without distinction of VRs or VPNs. It is up to the ISP to run queries on the shared logs to extract the correct data for each customer. With some Vendors this went to such an extreme that even the different types of logs were put together and the ISP would end up with Firewall logs, VPN services logs, routing logs, hardware logs etc… from all Virtual Routers of all VPNs running on the same device in one single file. Needless to say that in such scenarios when an incident occurs, it is impossible to analyze logs manually and security and network experts know how valuable logs are. Fortunately, most Vendors have resolved this issue not only by allowing the separation of logs in a more or less detailed way but also by supplying software to Providers in order to deliver reports to their end-users.

The management done by the ISP is always done out of band, however the management functionalities for the customers as well as the reporting to the customer could be done in two ways: In band vs. Out of Band.

“In band” and “Out of band” actually refer to the path used to transport the Packets.

In the above scenario, “In band” management and reporting would signify that the management and the reporting are done through the customer VPN itself, without having to use the public Network. This means that the reports need to be delivered on a server inside the customers VPN and a management console needs to be provided on

[13] Redback Networks. URL: http://www.redback.com/en-US/products/no_se_datasheet.html

one of the Customer premises Local Networks. An example of "in band" management would be to extend each customer's VPN up to the ISP's data center in order to provide direct access to a dedicated web server to which the ISP would upload reporting data.

"Out of Band" means that reporting and management data is transported over the public Internet. In other words, additional security such as authentication and confidentiality needs to be provided. An example of out of band management would be a publicly available secured web server to which a customer can connect using SSL in order to modify his network configuration.

Although more complex to achieve, "in band management" is the preferred and more secure solution because reports or management devices are only accessible from within the VPN. Even though the traffic does not leave the VPN, authentication and encryption should still be foreseen in order to protect against internal attackers.

6. So which VPN should I take?

It is impossible to provide a generic answer to this question. The choice depends mainly on a company's network, but also on elements such as outsourcing considerations, company security policy, etc. Instead of answering the above question I would like to include a table that summarizes the major pro's and con's of Network based VPNs[14].

6.1. Pro's

- SLA's across the backbone
- Fully redundant equipment
- No experts required in-house
- Very cost effective
- New service activation nearly on the fly

6.2. Con's

- Limited design decision (standard designs)
- Shared platforms
- No good visibility on Configurations
- The Platform Vendor needs to provide all functionalities, it is very difficult to integrate 3rd party equipment (e.g. It would be very tricky to have a network based VPN and use a Nokia/Checkpoint Firewall Solution for internet break-out)
- Bound to one service provider

[14] Bryan, Meckley. URL: http://www.oft.state.ny.us/security/electronic%20presentations/conference2001/CPEvsNET_VPN.rtf

- Last mile is not secured

Basically, pros of Network based VPNs are the cons of CPE based VPNs and its con's are the pros of CPE based solutions.

7. Conclusion

Although the purpose of a VPN is always the same, the methods of implementing it are only limited by the creativity of its designers and the budgets of companies. The solution I have provided is only one of many possibilities within network based VPNs. The principle of Network-Based VPNs relates to the location of the "VPN Device". In a network based VPN the intelligence and the processing power are on the Edge of the ISP's backbone. This requires a total re-thinking and sometimes challenging designs known as "best-practice" solutions, not only in network security, but also in network design in general.

From an ISP's point of view, Network Based VPNs enable them to provide standard, scalable VPN solutions. Thanks to management tools provided by vendors, the manageability of multiple large VPNs as compared to CPE based VPN improves exponentially and as management is easier, there is less risk of errors and security breaches. The biggest danger of network based VPNs is a badly secured management network.

From a customer's point of view, Network Based VPNs are the ideal solution to avoid all the hassle of building a virtual private network in-house and this at a competitive price. On the other hand, it requires an even better preparation phase where security policies, SLAs etc… need to be developed in order to properly evaluate the different solutions proposed by the outsourcers.

As network based VPNs run on shared equipments, they make it more complicated to implement principles such as the "Principle of least Privileges" and "Defense in Death".

8. Glossary

VPN	Virtual Private Network
ISP	Internet Service Provider
CPE	Customer Premises Equipment
FW	Firewall
NDA	Non Disclosure Agreement
SLA	Service Level Agreement
DMZ	Demilitarized Zone
DNS	Domain Name Services
RAS	Remote Access Server
IETF	Internet Engineering Task Force
SSH	Secure Shell
API	Application Programming Interface
VR	Virtual Router

9. References

1. Tim, Greene. “IP VPNs are a top choice for WANs, study shows”. December 31 2002 URL:http://www.nwfusion.com/newsletters/vpn/2002/01674562.html (January 15 2003)
2. Cosine Communications. “Moving Into the Cloud: The Case for Network-based VPNs”. March 2000. URL:http://www.adimpleo.com/library/cosine/cosinewp.pdf (January 9 2003)
3. David, Willis. “The next revolution in VPNs” August 5 2002 URL: http://www.nwc.com/1316/1316colwillis.html (January 15 2003)
4. Bryan, Meckley. “IP-Virtual Private Networks CPE-based vs. Network-based”. April 24 2001 URL:http://www.oft.state.ny.us/security/electronic%20presentations/conference2001/CPEvsNET_VPN.rtf (January 14 2003)
5. Corona Networks. “Delivering Next Generation IP VPN Services”. February 2002 URL:http://www.coronanetworks.com/products/whitepap/documents/NextgenIPVPN.pdf (January 15 2003)
6. David, Holdes. “The ATM and IP report guide to IP Service Switches” April 2 2001 URL:http://www.broadbandpub.com/broadbandworld/v3n2/survey2.pdf (January 15 2003)
7. Synthil, Chetty. “Outsourcing Security Management.” April 9, 2001. URL:http://www.sans.org/rr/policy/outsourcing.php (January 9 2003)
8. IETF Workgroup. “IP Security Protocol (ipsec)”. October 10 2002. URL: http://www.ietf.org/html.charters/ipsec-charter.html (January 14 2003)
9. Jessica, Yu. “Network based IPVPN Architecture using Virtual Routers”. February 19 2003 URL:http://www.nanog.org/mtg-0102/ppt/yu.ppt (January 15 2003)
10. Futuresoft. “Virtual Routers, Why Where and How” URL: http://www.futsoft.com/pdf/Virtroutwp.pdf (January 16 2003)
11. Corona Networks. “Multi-Service Virtual Routers”. May 2002 URL:http://www.coronanetworks.com/products/whitepap/documents/CoronaOS%20White%20Paper.pdf (January 15 2003)
12. Cosine Communications. “CoSine Communications and Check Point Team to Deliver Integrated VPN and Firewall Services From Within the Service Provider’s Network”. June 5 2001 URL:http://www.cosinecom.com/newsevents/pressreleases/20010605.html (January 14th 2003)
13. Curt, Newton. “Virtual Routing promises new IP Services”. (April 16 2001) URL:http://www.nwfusion.com/news/tech/2001/0416tech.html (January 15 2003)
14. Redback Networks, “NetOp SmartEdge Management Suite”. Date unavailable URL:http://www.redback.com/en-US/products/no_se_datasheet.html (January 15 2003)

Last Updated: August 19th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Adelaide 2017	OnlineAU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced