Global Information Assurance Certification Paper

Corporate Remote Access VPN: Issues and a Solution

By: Stephen Pedersen

The reason for the trend:

The "Internet Revolution" has spurred home PC users to connect their computers to the Internet. The vast amount of information available, at anytime and the new e-business economy has contributed significantly to this trend. In recent years, the advancement of technologies like cable modems and digital subscriber line (DSL) have dramatically reduced the cost of High Speed Internet Access to consumer prices.
Many organizations are deploying IP base applications and corporations are ready to take advantage of broadband Internet access for two reasons. The new e-business economy is highly competitive and profits are shrinking. By deploying **R**emote **A**ccess **VPN** (RAVPN), companies can reduce the cost of traditional RAS servers and modem pools. Secondly, company may enjoy increased productivity from their employee's. The users have taken to this idea because it allows for flexible work schedules and telecommuting means no more rush-hour travel. All of these reasons add momentum to the use of RAVPN.

The flip side of the coin:

Broadband Connectivity

Broadband Internet connectivity, also know as "always on" access, has many advantages, but at a cost. There is a significant threat to corporate LAN security. Security is only as good as the weakest link. Many of the PC's used for RAVPN are win9x based machines. These systems are notorious for their poor security and most of these PC's are configured by novice users or are purchased with a vendor's pre-configuration already installed. Neither of these configuration have any consideration for the system network security in mind.

Anti-Virus Software

Computer viruses have been around for a while now and most users have some form of anti-virus software installed. In today's hostile Internet environment, anti-virus software alone is not sufficient. More advanced security applications are required to maintain the security and the integrity of the system connected to the Internet. Anti-virus software is still very important and the dilemma of keeping virus signature file up to date is still one of the RAVPN administrator biggest challenges. This year, 2000, has been no exception. We have seen email viruses, like "ILOVEYOU" and "MELISSA" spread at exponential rates, bringing email systems to their knees.
Distributed Denial of Service (DDOS) has been able to take large e-commerce sites down. These sites have invested huge amount of money into security and have still been susceptible to attacks. In a nutshell, the DDOS attacks are possible because of the vast number of insecure PC's connected to the Internet. These systems have been compromised and a Trojan-horse application installed. The hacker then has control over

this system from a central location and can instruct many thousands of system to establish rogue connections to a server simultaneously. This will consume the resource of that server and therefore it will not be able to respond to legitimate connection requests. Lance Splitzer's recent article entitled "Know Your Enemy:Worms at War" is a great testament to how rampant the Trojan-horse applications problem are. (For details see Reference)

Trojan-Horse Applications

The biggest concern for the RAVPN administrator is the threat of a client being infected with one of the many remote control Trojan apps that are floating around the Internet. When the infected client connects to the "Secure" corporate LAN via the RAVPN, the VPN server will consider this client a trusted entity. But a hacker maybe able to gain unrestricted and undetected access to the LAN via this Trojan application. All traffic will appear to the VPN server as coming from the trust client but may actually be from the hacker using this remote control Trojan.

A variant of this kind of attack was recently demonstrated when Microsoft was hacked with the use of the QAZ Trojan. (See Reference). The users RAVPN authentication credentials were stolen and then used to gain access the LAN via the RAVPN as a legitimate user. The lessons that stand out in this article are the vulnerability of PC's connected to the Internet and the need for strong authentication methods, like SecurID and PKI.

Split Tunnelling

The attacks described above are possible because of split tunnelling. Split tunnelling is when a system can build a VPN tunnel to a Secure Site and continue to access other networks outside of the VPN tunnel, moreover other system can access the system that has an established VPN tunnel. There are pros and cons to this type of configuration. The cons we have already covered. Tim Greene wrote an article discussing the benefits of split tunnelling in detail. (Reference below) To sum up the benefits, split tunnelling will allow a busy telecommuter to access information on other networks with out having to tear down the VPN tunnel and then have to re-establish the tunnel to continue access resources within his office LAN. Split tunnelling would also keep unnecessary traffic off the corporate Internet access and VPN server. If the traffic is not required to be secure, why waist CPU cycles dealing with encrypting and decrypting this traffic.

A Possible Solution:

Scope of Solution

I will summarize what we have discussed above as the requirement for our solution:

1. Support Windows 9x, WinNT 4 and Win2000 Clients
2. Build a Secure Remote Access Service using VPN technology from the Internet.
3. Must be usable with dialup access (Road warriors) and broadband access (Telecommuters)
4. Must have Anti-virus capabilities with regular/automated updates
5. Client side firewalling with centralized policy control
6. Client side firewall policy verification
7. Revoke a users access and deny access for invalid client firewall policy
8. Make use of Strong Authentication methods
9. Flexibility to allow or disallow split tunnelling

Out of Scope

1. Sizing of hardware
2. Redundancy and High Availability
3. Multiple Entry Points
4. Other Client Operating Systems
5. Deployment of Client Software
6. Intrusion Detection and VPN server Integrity

Solution Components

1. Sun Microsystems server(s) running a stripped down harden install of Solaris 2.6
2. Check Point VPN-1 V4.1 Service Pack 2
3. Check Point SecureClient/SecuRemote V4.1 Service Pack 2
4. McAfee Virus Scan V4.5.0
5. RSA SecurID Server

Putting it together

We built a Solaris server from a Solaris Jumpstart server. The jumpstart profile has been tailored for this purpose. Only the necessary Sun packages are installed and all services are disabled. We added Secure Shell for network access and an Empire snmp agent to allow for real time surveillance and to trend server performance and health statistics. The jumpstart also installed VPN-1 and its service packs as well as a pre-configured SecurID client. The jumpstart server allows us to duplicate this configuration with very little effort. The jumpstart does not configure VPN-1 software this is a manual process. We will not going the detail of configuring VPN-1, there are numerous documents on Check Point's website that can help you with this. The VPN-1 server is licensed appropriately

and a policy server license is also added. The policy server is responsible for the clients firewall policy and is also used to verify the policy on the client. Today we have four choices for the policy options on the client.

1. Allow Any
2. Allow out bound connections only
3. Allow only Encrypted traffic
4. Allow Encrypted traffic and out bound connections

Configuration Verification Options:

1. Desktop is Enforcing Required Policy
2. Policy is Required on all Interfaces
3. Only TCP/IP Protocols

The VPN server is configured with a public IP address on the Internet side and a private (RFC1918) IP address on the LAN Side. A 2nd firewall was built using the same jumpstart profile and instal outside of the VPN server. The external interface of the VPN server is connected with a crossover cable to the outside firewall, a defence in depth strategy. The outside firewall policy only allows the Internet to talk to the VPN server on the following services: IPSEC, CheckPoint's RDP and fw_topology (tcp 264).
The SecurID server is located on a very secure segment of the internal LAN. The LAN IP address of the VPN server is registered with the ace server as a client. A SecurID user group is created and added to the VPN servers object. This allows us to add/delete individual users from authenticating from the VPN server IP address, causing the desired effect of centrally controlling individual VPN user access.
VPN server policy/ruleset is managed by an enterprise VPN-1 management console. It is preferred that the management console be separate for a number of reasons. Firstly, if the VPN server is compromised the policy cannot be change. Secondly, logging will then be collected on a server other than the VPN/FW server and if multiple VPN servers exist, the logs will be in a single location. Log processing requires CPU and we don't what to bourdon the VPN server with this task. The VPN server is configured with a single generic user, called generic*, with SecurID authentication. This means all user authentication requests will be forwarded to the SecurID server. The net effect is users only have to be defined in the SecurID server and added to the newly created SecurID group. The generic* user is added to a group called vpn_users, this is a group on the VPN server and not the SecurID server. We can now configure the VPN gateway object for encryption, defining the local LAN address space as the encryption domain and add the rule to allow the VPN tunnel.

Source	Destination	Service	Action	Log
Vpn_users@Any	Localnets	Any	Client Encrypt	Log Long

Client Side

On the client we installed the anti-virus software and configured the auto update feature from the Virus Console. Two servers were added for all clients. The first was an internal server on the LAN and the second was the Network Associates server. Both servers use anonymous ftp to get the latest signature update. This configuration will allow notebook uses to get the update while in the office or on the Internet at home.
The VPN client software is installed with a preconfigured site and in Secure Desktop mode; Secure Desktop enables the firewalling capabilities of Check Point VPN client. Now we are ready to used VPN.
When a user tries to access a LAN resource, Secure Client will pop up a VPN authentication window. The user can enter his/her SecurID userID and passcode.
After the user is authenticated, the VPN server will then verify the client's desktop security policy with the current policy on the Policy server. If these policies match the defined verification options, the access will be granted to the resource via the VPN tunnel. If the policy does not match the Policy server will display a messages to the client to this effect and ask if the client would like the policy server to install the correct desktop security policy. If the user accepts this request, the policies will match and the VPN tunnel is allowed. The secure VPN session is established.

Conclusion

We have created a secure vpn solution that supports all the required clients with anti-virus software that automatically updates its signature file. All clients have basic firewalling capability, which is controlled and verified by the policy server. The policy server gives us the flexibility to control split tunnelling and different levels of policy verification. All users are centrally managed and use token-based authentication.

Reference:

- Check Point Software and VPN-1 Secure Client
  http://www.checkpoint.com/products/vpn1/secureclient.html
- Know Your Enemy: Worms at War By: Lance Spitzer, 11/9/00
  http://www.enteract.com/~lspitz/worm.html
- Intrusion Detection for FW-1 By: Lance Spitzer, 11/1/00
  http://www.enteract.com/~lspitz/intrusion.html
- Tunnel Vision By: Curtis Dalton July 00
  http://www.infosecuritymag.com/july2000/tunnelvision.htm
- Cable Modems and Corporate Security By: Ed Pardo, 03/21/00
  http://www.sans.org/infosecFAQ/cable.html
- The benefits of split tunnels By: Tim Greene, 08/25/99
  http://www.nwfusion.com/newsletters/vpn/0823vpn2.html
- MITNICK: Microsoft hack wasn't espionage By: Kevin Mitnick, 11/5/00
  http://www.securityfocus.com/commentary/112

Last Updated: October 22nd, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive