Global Information Assurance Certification Paper

Paul D. Warnagiris

Security Essentials GSEC Practical Assignment Version 1.4b, Option 1

11 August 2003

Protecting the Enterprise While Allowing Remote Access

Abstract:

In today's information age it is imperative to allow users to work remotely. "It is estimated that 30 million U.S. workers telecommute at least some of the time."[1] Simply setting up a client-to-site Virtual Private Network (VPN) may, at first glance, seem to be the answer. The question is, does a client-to-site VPN alone solve the problem or create larger problems? Simply allowing access to your internal corporate network from remote desktops or laptops solves the problem of allowing remote access, but it opens your protected network to numerous potential vulnerabilities.

> "One way to think of a VPN is as a hole in the firewall. Someone with a VPN is allowed to tunnel through the firewall into the network," Counterpane's Schneier says. If a VPN user has an always-on Internet connection like cable or DSL, it complicates things. His or her system is connected to the Internet and if it is unprotected (read: no firewall) it becomes an easy target."[2]

In essence by allowing remote access into your corporate network your security is only as good as the security of the remote system. Security of most home users' systems is laughable at best. If a remote user's system is compromised and it has direct access to your protected network, the chances are good that your protected network will be compromised as well. There are policies that need to be put in place as well as procedures that need to be followed. This paper will take a two phase approach. It will discuss policies and procedures that need to be in place and make recommendations in order to do remote access correctly. It will also discuss various technical ways of protecting remote laptops as well as a step-by-step configuration guide to Checkpoint's SecureClient.

[1] Hesseldahl, Arik. "Trojan Horse, Meet The Home Office." 15 July 2003.
URL: http://www.forbes.com/2003/07/15/cx_ah_0715telecommute.html
[2] Bertin, Michael. "The New Security Threats." 15 January 2001.
URL: http://www.zdnet.com.au/newstech/security/story/0,2000048600,20108148-2,00.htm

Variations of remote users

There are a few different ways that remote users can connect to the corporate network while they are not in the office. One way is by dialing into a RAS server. By doing this the firewall is completely circumvented and the speed of the connection cannot be faster than the analog line the remote user is dialing in from. Another way to connect – one of the most popular and cost-efficient ways – is via a client-to-site VPN. The client-to-site VPN gives the end user as much functionality as if he/she were sitting in the office. It is also one of the most cost-effective methods because it utilizes the public internet. It can also be one of the most dangerous ways if there are not policies and standards in place to dictate which types of computers are permitted to connect and how they must be configured when they are connected. "On the technical side, the rise of always-on connections such as DSL (Digital Subscriber Line) and cable at home means users will tend to leave connections open more. Without a personal firewall, such a computer is a gaping hole for an enterprise."[3] This is not to say remote access cannot be done securely, but in order to do remote access there will need to be policies in place as well as technology implemented to help bolster enterprise security.

Often home computers are given access to the corporate network under the assumption that personal firewalls provide adequate protection. This is not always the case. To assure that network security is not compromised, one must consider a few important questions. Who implemented the firewall? Is the firewall always turned on? Is the firewall configured correctly? If there are problems accessing certain files or programs, would shutting off the firewall be the first fix?

Remote access from corporate computers only

No matter what industry you are in, if you do not have a policy in place that states there will be no home computers allowed to access the corporate network, your security will only be as good as the least secured computer in your extended LAN. This line item in the security policy should be very close to the top. This policy reform may elicit complaints, but home computers should be prohibited from connecting to the corporate network in all cases. Granted, implementation of this policy will cost the company more money. If the company wants employees to work from home, it will need to supply them a corporate laptop or desktop. If the company does not want to bear this expense, then it must not expect employees to work from home.

Technology writer Jessica Hirsch reinforces this point in her essay, "Telecommuting: Security Policies and Procedures for the 'Work-From-Home' Workforce."

[3] Berinato, Scott. "Telecommuters: Threat to Security?" 20 November 2002.
URL: http://www.zdnet.com.au/newstech/security/story/0,2000048600,20107188,00.htm

> "Any business with a number of dedicated telecommuters needs to seriously consider purchasing or leasing the equipment for their employees, or sharing the cost of the hardware. An American Management Association survey in November 1999 found that 42% of telecommuters were using personally owned technology to access business networks. Generally speaking, these computers are not subject to many of the "appropriate personal use" clauses in telecommuting policies, may contain conflicting or malicious software, are not thoroughly audited on a regular basis, and eliminate much of the control that a company's IT department has over telecommuting and the security thereof. Though the cost of ownership of this hardware may be higher, the trade-off of increased security and control may be worth it."[4]

The company could have a secure alternative that does not require the purchasing of new equipment. If the employee hands over his/her computer to the IT/Security team, the team could re-image the desktop. This would allow the employee to connect remotely without compromising network security. This of course would mean that the 'corporate' build would be employed on the employee's home desktop and the entire system would be wiped away. The desktop would then be secured as if it were a laptop going out into the field. The Employees would no longer have administrative privileges on their own home desktops (as we will discuss later in this paper). This is a choice you can give the users rather than just saying "no." While many users may find these options restrictive, a secure network demands security at all points, at home as well as at the office.

By adopting a zero-tolerance policy you can protect your network from the security lapses of the traveling road warrior who might think it harmless to allow his/her son to download internet games onto a computer that is connected to your corporate network. Addressing this issue will take care of a common weakness prevalent in corporate networks. However, it still is a long way from securing your enterprise from remote user compromise.

All boxes that connect remotely must be under the complete control of the Corporate IT team

Only computers under the complete control of corporate IT should be allowed to connect remotely. This mandate is another important item of security policy. It will not help your security in any way to secure remote laptops/desktops and then turn around and give those remote users administrative privileges. Administrative privileges on a laptop are akin to root on a UNIX box. Anyone with root/administrative privileges can circumvent any and all security measures put in place.

---

[4] Hirsch, Jessica L. "Telecommuting: Security Policies and Procedures for the 'Work-From-Home' Workforce." URL: http://www.teleworker.org/articles/telework_security.html

Mandating the Corporate IT team to be in charge of the remote computers doesn't help the situation if there are no policies and procedures in place to guide that team. The type of enterprise you are trying to secure should dictate how strict or lenient your policies are. In your policy you can mandate anti-virus protection on each computer. You can set guidelines requiring the updating of such policies, and you can require a personal firewall running on the computer; however, you cannot make the users responsible for maintaining their laptops or the security of their laptops. If the Corporate IT team does not have complete control of the laptop they cannot secure it nor can they guarantee the security and integrity of the corporate enterprise.

Tips for securing home/remote users[5]

- All remote users should have a personal firewall. Not only will it protect the computer from invasion but also will tell you how many times the connection is being probed.
- All remote users should have intrusion detection systems to provide an additional layer of information on break-in attempts.
- The company's IT team should set up the home system instead of letting the user buy something, expense it and set it up themselves. That will give you the chance to take care of vulnerabilities and harden up the system.
- Make sure the IT team is responsible for installing patches and software upgrades for home users.
- Computer policies in effect in the office also should hold the same for telecommuters and travelers, if not more strict. If company computers aren't to be used for personal use in the office, the home user shouldn't be surfing the 'Net or letting kids play games on the company system.
- Monitor what software is being installed on the remote system and restrict it to business use only. Do not allow software to be installed unless it is installed by Corporate IT
- The IT team needs to check these systems with the same due diligence it does systems in the office, even if it means doing periodic visits.
- The traveling worker needs to have sensitive files encrypted.
- Install access control programs that will ask for a password and then alert an administrator via modem if that password is being put in incorrectly.

[5] Gaudin, Sharon. "VPN vulnerability." 14 August 2000.
URL: http://www.nwfusion.com/research/2000/0814featsidethree.html

- Traveling workers should be reminded not to leave computers in hotel rooms or cars. Don't let a system with a VPN into the company network out of your sight.
- Traveling workers also should have multiple layers of security, such as screen locks and boot-up passwords.

Set policy that governs the build of remote systems

1. Remove administrative privileges. Any security that is put in place can easily be undermined by a user with admin privileges.
2. Limit remote users to the 'domain users' group if at all possible. Do not give more privileges to a user than absolutely necessary. This might cause animosity because users will not be able to install programs or even add a printer, but it is imperative to a good security policy.
3. Users must not install/load any program that is unknown to the Corporate IT team. If a program is deemed 'needed' by the user and management buys off on the issue, the application should be tested in a lab scenario before it is added to the remote user's build in order to ensure there are no conflicts with other applications or processes.
4. Remove access to the TCP/IP properties. There should be no reason for a user to change any TCP/IP settings. It is very unusual for a user to connect to a network where there is no DHCP. (We will see why this is important later in this paper when we discuss configuring SecureClient).
5. Remove the ***'connections'*** tab from the ***'tools'*** > ***'internet options'*** pull down menu from Internet Explorer. This will ensure there aren't any additional dial adapters installed that the security team is unaware of.

One of the biggest arguments for admin privileges on remote users' computers is just that: they are remote users. We cannot possibly foresee every situation a remote user will encounter, and that provides their argument for giving them admin rights. This is a valid observation, but unfortunately not reason enough to warrant admin rights. In order for the security team to properly secure the enterprise, the team must be in control of every aspect of that network. By giving admin rights to remote users you are effectively cutting the authority of the group that was specifically designed to administer and help secure your network.

Rules are meant to be broken

Of course there are going to be instances where it is not feasible to remove admin privileges. Most likely anyone that is technical on the staff will need admin privileges. Users that travel from site to site doing maintenance on the systems

will need to change their IP address as well as install programs needed to do their job. These users must be considered on a case by case basis. We will assume that a technically savvy person will be more security-aware and could be given more wiggle room. (Before you become enraged and protest the last statement, realize that I am comparing technical people to sales people. I'm not saying that technical people will not do things that are insecure, but they will do it knowing they are doing something insecure). This is not a steadfast rule and that is why every person granted elevated privileges should be considered alone and not as part of a group. Just because a person belongs to a specific group does not mean they should automatically gain elevated privileges. Along with escalated privileges should come a stern reminder that the amount of access and privileges given to said user is enough to compromise the system. If users are found gambling with the integrity of the network, they should have their rights limited, they should be reprimanded, and they should possibly be terminated. It is absolutely imperative to make this point very clear.

Protecting the laptop from intruders at all times

Protecting the laptop while it has a current session open into the corporate network is necessary for obvious reasons. Once the user disconnects from corporate and continues surfing on the web, this does not mean your responsibilities end. It is more likely that the user needs more protection while they are not connected via VPN because it is at this time that the user would be surfing unfavorable sites. Since the user knows that Corporate IT is watching while they are VPN'd in, they will most likely disconnect the VPN and then continue on to the dark side of the web (sex/gambling/drugs, etc.) This is where the protection is needed the most.

Personal firewalls come into play here and do a great job of securing unprotected laptops from outsiders. An example of a personal firewall is something along the lines of Black Ice, Zone Alarm or Symantec's personal firewall.[6] As explained above, control over these personal firewalls must not be given to the user. Personal firewalls can break connections such as certain types of streaming, file sharing and file swapping such as Napster and KAAZA as well as any type of instant messenger direct connect or any service that utilizes high order ports. For this reason users cannot be given control. If Charlie's IM video session home to his daughter is not working and turning off the firewall will fix the problem, Charlie will simply turn off the firewall.

Black Ice and Zone Alarm work well here, but can become cumbersome. There is a solution that gives the security admin, total control over the remote laptop. Let's say for example that everything is working well with your five remote users and you can sleep well at night knowing that your remote users as well as your corporate network are secured better than most. When you come in to work on

---

[6] Borch, James R. "Desktop firewalls put a shield around remote users." 29 August 2000. URL: http://archive.infoworld.com/articles/es/xml/00/09/01/000901esh2h.xml

Monday you hear the news that your company, Company A is merging with your competitor, Company B. Company B has 50 remote users because all of their salespeople are road warriors whereas your salespeople usually work from within the office. All of a sudden you realize that you now need to manage 55 different personal firewalls. There are centrally managed personal firewalls, but most are not cost-effective for a small number of users or are not robust enough.

One way to eliminate the problem of centrally managing the remote desktop security policy is to use vendor-specific applications that pushes a policy down to the remote user's computer the first time they connect and updates that policy subsequently each time they connect afterwards. If a remote user connects to the corporate firewall or VPN concentrator it will receive a policy that governs exactly what that box can do while it is connected to the corporate network. The great part about this solution is that once the user disconnects, the policy that was recently updated still remains on the remote computer. Once the user disconnects he/she obviously loses access to the corporate network, but while they are just surfing on the internet, their computer is locked down from external probes and attempted access. Two of the popular vendors that currently employ these features which are integrated in their firewalls today are Checkpoint and Cisco. Cisco uses its own proprietary client that is loaded on the remote computer that protects the computer at all times. Checkpoint works in the same fashion with it proprietary software called SecureClient.

Managing remote users desktop security by deploying SecureClient

SecureClient is an added feature that can be purchased from Checkpoint. When you purchase a CheckPoint firewall you do get a VPN client by default for no additional charge. The client that comes for no cost is called SecuRemote. SecuRemote works fine, but it only allows you to encrypt access to and from the corporate network. It will not protect the client. If you use SecuRemote, be sure to secure the client with some type of personal firewall at all times.

When you purchase the SecureClient add-on from Checkpoint you receive a license that permits you to enable the policy server on the firewall. This policy server allows you to make policies specific to different groups that will connect to your firewall. SecureClient also has some very handy features unavailable with SecuRemote that will help you secure your remote clients.

Secure Client Verification (SCV)

By utilizing SCV you can ensure various policies are followed. Even though it is possible to circumvent some of the security settings in SCV while a client is not connected to the enterprise, the next time that client attempts to connect to the corporate network it will be greeted with the message that states the client security settings cannot be verified and for this reason you will not be able to connect. You will now know that someone or something has changed the settings on the client for one reason or another. At this point you need to make a

decision; do you walk the user through reconfiguring the laptop correctly and possibly permit a compromised laptop on your network, or do you have the user return to corporate and re-image the laptop? This question needs to be answered by senior management and should be determined on a case-by-case basis.

Of course if the user wanted to get around the security settings, he/she can simply turn off SecureClient, do what they need to do and then turn SecureClient back on. In order to ensure this is not a possibility we need to refer to our security policy that states users cannot have administrative privileges. Without administrative privileges the user cannot disable SecureClient and therefore you are assured the client has been protected at all times. Some of the settings that are checked by the SecureClient Verification setting are as follows:

1. Apply SCV or do not apply SCV
2. Ensure the Secure Client policy is installed on all interfaces
3. Only allow TCP/IP protocols to be used

Applying the SCV policy ensures that only securely-configured laptops are permitted on the network. Ensuring the SecureClient policy is installed on all interfaces protects the enterprise in two different ways. First, it ensures the users did not install an AOL dial adapter (or similar) or a special cable modem adapter in order to surf the web through a different interface and circumvent the security policies put in place by SecureClient. If they did so they would be unprotected on the web and possibly compromised. The next time they connected to the corporate network there may be a compromised box with direct access to corporate resources. Second, it ensures that the user simply did not disable the SecureClient adapter from a known working adapter such as the wireless adapter or the built-in NIC on the laptop in order to do what they needed to do. Of course the user would not be able to disable the adapter without admin privileges, but they can install another adapter though Internet Explorer from the connections tab even without admin privileges. For this reason it is recommended to remove that tab via the use of a group security policy pushed down from the domain controller. This is just one option that can be utilized through the GPO function. Group security policies are outside the scope of this paper, but are very necessary in securing remote users. For more information regarding the configuration of group policy please refer to http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx and download the whitepaper.[7] There is also an option in SCV to allow only TCP/IP protocols from the client to the corporate network. Depending on the setup and the specific business needs you may or may not want only TCP/IP protocols to

7 Lundy, Jim. "Administering Group Policy with Group Policy Management Console." "GPMC_Adminstering.doc" April 2003.
URL: http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx

be permitted from remote clients. SecureClient configuration violation notifications can be configured to generate an alert in the client log as well as the firewall log, to notify the user via a pop-up or both.

Configuring SecureClient step-by-step in a stand-alone environment

1. Licensing the firewall for SecureClient

Licenses for SecureClient come in a variety of number of user options with a minimum of 25 and a maximum of unlimited**.** Once you obtain the correct license(s) they will need to be installed on the enforcement point as well as the management module in a distributed environment. The two licenses are very similar and if you are not exactly sure which license to place on which module, keep in mind the following: On the management station you need to place the license with the "CPVP-VPS" in the string. On the enforcement points you will need to place the license with the "CPVP-VSC" in the string. If you only have a stand alone environment there should be no problems applying the license.

2. Enabling the Policy Server:

Once all of the modules are successfully licensed the first thing that must be done is to enable the policy server. In order to do this you must check the box that reads ***'SecureClient Policy Server'*** in the firewall object's 'properties' page. You can access the properties of your firewall object by opening ***'Network Objects'*** and then ***'Check Point'*** from the ***'objects tree'*** in the policy editor. To display the objects tree simply go to the ***'view'*** pull-down menu and select ***'objects tree.'***

3. Configure global property settings

From the ***'policy'*** pull-down menu in the policy editor (AKA Check Point SmartDashboard) select ***'global properties.'*** Select and expand the ***'remote access'*** branch of the tree. Click on the ***'update topology every X hours'*** and define a value for the amount of time a client will go before it updates its policy. Directly below that check box you can select ***'Automatic update'*** or ***'Upon Startup.'*** If you select ***'Upon Startup'*** the remote user will be prompted each time he/she starts his/her machine within the course of the X value that was set. If ***'Automatic Update'*** is selected it will be transparent to the user. The defaults can remain for the rest of the selections on this page with the exception of the ***'Encrypt DNS Traffic'*** box. If the clients that will be connecting remotely are going to use internal DNS in order to operate (they most likely will), then this box needs to be checked. Even if you tell the firewall to permit and encrypt DNS, if this box is not checked it will not be encrypted. This is a very simple step to overlook when you are setting up SecureClient. Also, there is an option to cache passwords on the desktops. Do not select this option for obvious reasons.

Next select the ***'VPN – Basic'*** branch of the tree. If you will be using pre-shared secrets for authentication methods, select the ***'pre-shared secret'*** box. In this paper we will be using certificates that are going to be generated by the ICA for remote clients (more on this later in the paper). Select the ***'Gateways support IKE over TCP'*** check box. This is necessary in this day and age because of the wide acceptance of NAT. It is more likely than not that one or more of your remote users will be NATted behind some sort of device. When IKE negotiations occur, they involve sending UDP packets, which under certain conditions generate multiple IP fragments. Some NAT devices are unable to properly translate IP fragments, which may lead to the loss of theses packets and cause communication failures. In order to overcome this problem Checkpoint allows you to select the ***'IKE over TCP'*** option and this will send IKE negotiations for Phase 1 over UDP instead of TCP, thereby eliminating the shortcoming of certain NAT devices. Further on this page you have the option of selecting IP compression for SecureClient which is self explanatory, and you also have the option to enable load distribution for Multiple Entry Point (MEP) configurations. This paper will not be demonstrating a MEP configuration.

Next select the ***'VPN – Advanced'*** branch. On this page you will define the encryption algorithm and data integrity that will be used. These properties will override any specific user setting that may or may not be configured. When selecting the encryption level, be sure not to violate any encryption export laws. For Data Integrity you may choose SHA1 or MD5. This will define the cryptographic checksum method used for ensuring data integrity. The IKE security association selection is next. There are three predefined groups; 768, 1024 and 1536. Keep in mind the larger the group the better the security will be; however, it will be more processor intensive. We will select group 1024 in our example.

Next select the ***'Certificates'*** branch. This will be an important branch because you will be generating certificates for each user that will connect remotely. By using certificates the user will not only need to know a password, but he/she must also be in possession of a certificate generated by the ICA in order to connect remotely. You can also use a two-factor authentication method such as RSA for authenticating a client. It is not recommended to simply use a FW1 username and password in order to connect to the corporate network:

> It's generally accepted that static passwords are insufficient where you don't have adequate compensating controls (such as physical security). They are particularly inadequate where you have any type of remote access, which includes Internet-based VPN's, dial-up, and WLAN.[8]

[8] Dodd, Paul. "A Technical Comparison of TTLS and PEAP." 29 November 2002. URL: http://www.oreillynet.com/cs/user/view/cs_msg/11775

Next select the *'client will verify gateway's certificate against revocation list.'* This will ensure the certificate the client is using has not been revoked. Also click the *'renew users internal CA Certificates'* box. The default of 60 days before expiration is acceptable in this example.

Next select the *'Secure Configuration Verification (SCV)'* branch. It is here you will configure the SecureClient Verification policies as described above. Once that is complete you can click *'OK'* to exit and save the global properties changes that have been made.

Firewall properties configuration

From the *'properties'* menu of the firewall object select the *'VPN'* branch. Select the *'traditional mode configuration'* button. Under the *'Support authentication methods'* section select the *'Public Key Signatures'* checkbox and then click on *'Specify'*. Ensure that *'The gateway can use any of its certificates'* radio button is selected and click *'OK.'* Also ensure the *'Exportable for SecuRemote/SecureClient'* checkbox is selected and click *'OK.'*

Next select the *'VPN Advanced'* branch. Ensure that *'Support NAT traversal'* is checked and *'VPN1_IPSEC_encapsulation'* is showing in the pull-down menu.

Next select the *'Remote Access'* branch. Select the radio button for *'Allow Office Mode to all users.'* By doing this, all remote users will receive an internal IP address (different from those used on your internal network by internal machines) when they first connect.

> Office Mode (OM) enables the organization to assign internal IP addresses to SecureClient users. This IP address will not be exposed to the public network but will be encapsulated inside the VPN tunnel. This mode allows an administrator to control which address will be used by remote clients inside the local network and thus make them part of the local network.[9]

If the remote users were not to get an internal IP, all internal servers would have to accept connections from all IPs. It would appear that externally routable IPs were accessing your private network because without OM enabled, they would be passed through by the firewall. By using access-lists or host.allow files, you strictly limit the users that can connect to any internal servers without limiting legitimate user access. It is possible to setup a DHCP server to dole out IPs to remote clients as well as defining a network range and letting CheckPoint hand out the IPs. In this example we will let Checkpoint do the DHCP. Select the

[9] "Checkpoint Desktop Security Guide." November 2002.
URL: http://www.checkpoint.com.cn/azgl/Desktop%20Security%20Guide.pdf (Page 171).

'manual (using IP pool)' radio button and click the *'optional parameters'* button. Here the DNS and WINS servers can be defined along with the domain name. Select the correct objects for the respective servers and click on *'OK.'*

Next select the *'Authentication'* branch. Ensure that all authentication schemes are un-clicked. At the bottom of this page under *'Policy Server'* select the group that will need to get a policy from the policy server. If you have not defined a group at this point, click the *'new'* button and define one now. Name it *'contact-ps.'* All users should contact the policy server in order to get a policy so this group will eventually contain every user that is defined.

Defining Templates

The easiest way to create users is by using templates. Before you can make any templates you will need to define some groups that your templates will use. In this example we will use three groups, *'sales,'* *'ops'* and *'helpdesk.'* Create these simple groups by right clicking on the *'groups'* tree branch under the *'users'* tab in the *'objects tree.'* Also make one more group called *'contact-ps'* if you have not already defined this group in the previous step. If you have you can use that group instead of creating a new one.

Next simply right-click on *'template'* under the *'users'* tab of the *'object tree'* and click *'new template.'* Name this template *'sales_template'* on the *'general'* tab of the template properties. Next select the *'personal'* tab. Ensure that the expiration date for this template is correct. Next select the *'groups'* tab. You will want to add the previously created *'sales'* group as well as the *'contact-ps'* group to the *'belongs to groups'* form the *'available groups'* box. On the *'authentication'* tab select *'undefined'* from *the 'authentication scheme'* pull down menu. Next select the *'encryption'* tab. Click on the *'IKE'* click box and then click *'edit.'* Ensure that only the *'public key'* box is checked and click *'OK.'* Next, click on the *'time'* tab. Here you can define the time of day this group can access the resources that are going to be defined by the policy. Finally, click on the *'location'* tab. Here is one place that you will define where this group of users will have access. In the *'source'* box leave the source of *'any'* and in the *'destination'* box add the networks the *'sales'* group will be able to access. Adding the destination network is a very easy step to skip, and if you do not enter the correct destination network it is possible that you will go bald trying to troubleshoot what is going wrong. There are three places where you must configure destination networks for SecureClient and this is one that is easy to forget about (the other two are the desktop policy and firewall rule base). Once you are finished with that click *'OK.'* Repeat these steps for the other two groups named *'ops'* and *'helpdesk.'*

Creating Users

Now that the templates are created it is time to create the users. In order to do this, simply right click on the *'users'* branch and select *'new user.'* Then, navigate to the correct template. If you are creating a new sales user, select the *'sales'* template. If you are creating a new ops user, select the *'ops'* template. In the *'general'* properties tab give the user a login name. All other tabs will already be filled out by the template. The only other tab that needs to be defined is the *'certificates'* tab. Click on it and then click on *'generate and save.'* This will generate the certificate the remote client will use in order to gain access. When you click on *'generate'* you will see a warning that tells you that once you make a certificate it cannot be undone unless you revoke the certificate. Just click on *'OK'* to that warning. Create an initial password for this user. Make it a unique password so all of the new certs you create do not have the same password. Enter the password a second time to confirm and then click *'OK.'* You will be prompted to select the destination to save the cert. Select the correct spot and save the cert. Continue to do this until all of your users are created.

Creating a Policy for Secure Clients

The final step is to create the rules remote clients must abide by. This needs to be done in two places. First, in the firewall rule-base you need to create rules that allow the clients to connect. In order to add your SecureClient groups in the source column of the firewall rule-base you must right click on the source and select *'add user access.'* From there select the group you would like to add. Your firewall rule-base should look similar to the graphic below.

Security - 062303 | Address Translation - 062303 | Desktop Security - 062303

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
1	Helpdesk@Any	Helpdesk_Allowed	Helpdesk_Prot_Allowed	Client Encrypt	Log
2	OPS@Any	OPS_Allowed	OPS_Prot_Allowed	Client Encrypt	Log
3	Sales@Any	Sales_Allowed	Sales_Prot_Allowed	Client Encrypt	Log

In order to make sure the desktop configurations are verified, double-click *'client encrypt'* from the *'action'* column and ensure the *'apply rule only if desktop configuration options are verified'* checkbox is selected. Now you have to create rules that will be loaded on the client that permit inbound and outbound actions from the client itself. The *'desktop security'* tab of the SmartDashboard is where these rules will be created. These rules will be defined as inbound and outbound from the client's perspective.

The rules will be configured exactly as they would in the regular FW rule base with one exception. In a normal firewall rule-base you will have one set of rules

that govern inbound and outbound traffic. In the desktop security policy you will have a set of rules that govern inbound traffic as well as a separate set of rules that govern outbound traffic. You must keep in mind while creating desktop rule-sets, the destination network in the rule-base must match the destination networks in the ***'user's property' 'location'*** tab which was defined during the template creation process.

One other very important thing to remember about the desktop policy is the no default clean-up rule. If you define the destinations and protocols that remote clients are able to use and you don't include an 'any-any-any-drop' rule at the end, the clients will be able to initiate any outbound connection to any network. This is not a good reason because if your client is already compromised or becomes compromised, it can use any outbound port to establish a connection. Your client may initiate a connection to a master server elsewhere on the internet that gives a black-hat remote control or shell access to your computer. As a general rule of thumb you should only allow needed outbound ports to be open. This is often overlooked by novice firewall administrators because they are only concerned with blocking inbound traffic. This could be a costly error.

Client configuration

This paper assumes the client is already installed on the remote user's computer. In the systray of the remote user's computer right-click on the SecureClient icon and select ***'configure.'*** From the ***'tools'*** pull-down menu select ***'log all blocked connections.'*** Also, from the ***'tools'*** pull-down menu select ***'client configuration mode.'*** Select the ***'connect mode'*** radio button. This will allow the client to receive a private IP from the firewall or the DHCP server in the corporate network. Click ***'OK'*** to save the connect mode changes. A reboot will be required.

It is now time to setup the site to which the client will connect. Ensure the client has internet connectivity. Be sure not to leave the client sitting on the internet for an extended period of time before getting a policy from the firewall. If you do so and there is no personal firewall on the computer, you are at risk of having the computer compromised before you secure it. The best case scenario would be to secure the laptop with a personal firewall before connecting to the Policy Server for the first time (this can cause connectivity issues for SecureClient if the personal firewall is blocking the connection) or connect to the firewall from a trusted interface.

You will need to move the cert that was created on the firewall to the client. It is best to transfer the cert by sneaker-net. Next, from the ***'sites'*** pull-down menu of the ***'Secure Client'*** window select ***'create new.'*** Enter the FQDN of your firewall or type in the IP address. You can also click on the ***'nickname'*** checkbox and give the site a friendly name. Next, click on ***'OK'*** in order to proceed. A ***'VPN-1 SecureClient Authentication'*** box will pop up. Click on the ***'use certificate'*** button. Next, browse to the place where the

certificate was saved. Once you have selected the cert, enter in the initial password that was designated at the time the cert was created on the firewall and click *'OK.'* You will be asked to validate the CA's fingerprint. The fingerprint was made when the CA was initialized on the firewall. If it is the correct fingerprint select *'OK'* once again. Once the grayed out *'OK'* prompt is able to be clicked, click it in order to save the updated data. You can now close the *'VPN-1 SecureClient'* box.

In order to launch the VPN, click one time on the SecureClient icon (envelope with a key) from the systray. Click on the *'connect'* button in the *'VPN-1 SecureClient Connection'* box. It will ask you once again for the password originally setup by the firewall administrator. Once you type in that password, instead of clicking *'OK,'* click on *'view certificate.'* At the bottom of the *'certificate'* box there is a button that says *'change password.'* Click on that button and change the password to a new strong password and click *'OK'* again. Click *'OK'* one more time to get out of the certificate screen and connect to the corporate network. In the dialog box you will see the client is contacting the policy server and you will see a successful completion of the VPN logon process if your laptop is securely configured.

Verify your policy

From the systray right-click on the SecureClient icon (it is now an envelope with a key flashing and a red and green lock blinking) and navigate to *'launch SecureClient diagnostics.'* This tool will show you if your machine is securely configured, allow you to read the logs of the client and show you the policy that was pushed from the corporate firewall. Even though there are multiple groups in the desktop policy on the firewall, once a client connects, the only rules that client will see are the rules that pertain to the group that client is in as well as the 'allusers@any' rule. The allusers@any rule is the default rule that will be in place on the laptop at all times whether connected to the corporate network or not. Ensure that you do have a policy and view your logs to see the client-side firewall in action

Follow-up

Allowing remote access into your trusted corporate network can be risky business. If you put policies and procedures in place along with current technology it is able to be done in a secure manner. Along with the policies and procedures that are in place it is also recommended that you audit those who follow the guidelines set forth. Ensuring that safeguards are used is as important as setting them up in the first place.

As always, the last thing that should be done before you are complete is to do a scan of your own network and remote clients. Use a program such as Nessus[10]

[10] http://www.nessus.org/download.html

or Nmap[11] to scan your enterprise network range and the public IP of your remote client. Ensure that the only ports open are the ones you know about. If you don't double check yourself to ensure there were no human errors, a black-hat will.

References

Hesseldahl, Arik. "Trojan Horse, Meet The Home Office." 15 July 2003.
URL: http://www.forbes.com/2003/07/15/cx_ah_0715telecommute.html

Bertin, Michael. "The New Security Threats." 15 January 2001.
URL: http://www.zdnet.com.au/newstech/security/story/0,2000048600,20108148-2,00.htm

Berinato, Scott. "Telecommuters: Threat to Security?" 20 November 2002.
URL: http://www.zdnet.com.au/newstech/security/story/0,2000048600,20107188,00.htm

Hirsch, Jessica L. "Telecommuting: Security Policies and Procedures for the 'Work-From-Home' Workforce." URL:
http://www.teleworker.org/articles/telework_security.html

Gaudin, Sharon. "VPN vulnerability." 14 August 2000.
URL: http://www.nwfusion.com/research/2000/0814featsidethree.html

Borch, James R. "Desktop firewalls put a shield around remote users." 29 August 2000.
URL: http://archive.infoworld.com/articles/es/xml/00/09/01/000901esh2h.xml

Lundy, Jim. "Administering Group Policy with Group Policy Management Console." "GPMC_Adminstering.doc" April 2003.
URL: http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx

Dodd, Paul. "A Technical Comparison of TTLS and PEAP." 29 November 2002.
URL: http://www.oreillynet.com/cs/user/view/cs_msg/11775

"Checkpoint Desktop Security Guide." November 2002.
URL: http://www.checkpoint.com.cn/azgl/Desktop%20Security%20Guide.pdf (Page 171).

URL: http://www.nessus.org/download.html

URL: http://www.insecure.org/nmap/

[11] http://www.insecure.org/nmap/

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event