GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

I. Summary: Virtual Private Network (VPN) technology has done wonders for the productivity of the common corporation. Using a VPN, companies can expand the reach of their corporate network beyond their expensive leased lines by using the assets provided by the Internet. This "reaching out" of corporate America has allowed for employees to securely access network resources while at home, allowed for secure partner communication, and decreased the costs necessary to do business. Instead of paying for expensive leased lines or incurring a productivity slowdown via usage of floppy transfer, employees and partners can now work remotely as if they were physically connected to the corporate network. Home users have begun to upgrade their home Internet connections to ISDN, DSL, and Cable allowing for greater speeds than ever before. These greater speeds allow for little speed penalty when telecommuting. Broadband connectivity seems like a perfect match to the corporate VPN world. It is a relatively low cost, high speed connection to the corporate network.

Alternatives:

Modem-Banks: Before the onset of high-speed Internet connectivity, many businesses relied upon huge modem banks to allow remote connectivity for their users. However, such solutions were prone to scans via a technique called War Dialing. This describes the usage of automated dialing software which methodically calls numbers in a pre-defined range or list, attempting to find a connection.[1] Although dial-up connectivity into Modem banks could be relatively secure, many systems were configured poorly and were protected with simple or no password. This type of connection was also fairly slow and very expensive if the connections were made via a long-distance carrier.

Leased-Lines: This type of connection describes a relatively static data connection between two points. The most common type of leased line is the T-1, a 1.544 Mbps connection (24 channel * 64 Kbps) [2] used by most businesses to enable consistent, high-speed connectivity between sites. Because of the high cost involved, usage of T-1s and the faster T-3s [3] generally used as company backbones but cannot be used for home access.

[1] Cowell, Ruth. *War Dialing and War Driving: An Overview,* June 11th, 2001
http://rr.sans.org/wireless/war.php

[2] Webopedia Article. *T-1 Carrier,* January 9th, 2002
http://www.webopedia.com/TERM/T/T_1_carrier.html

[3] Webopedia Article. *T-3 Carrier,* February 8th, 2002
http://www.webopedia.com/TERM/T/T_3_carrier.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Risk:

VPNs offer a perfect compromise between cost and speed, though they do so at considerable risk. When attached to a VPN a home (Intranet) or partner (Extranet) client the 'reach' of the internal network is extended to that client. Each time a user logs into the VPN the network is extended and the overall security and manageability of the network decreases. Each additional connection becomes another route to enter the internal network. Instead of managing only one major connection, that being the T-1/3 out to the Internet, the Security Engineer is now tasked with managing 5, 10, 20, 100, or even a 1000 concurrent connections.

The Goal: The scope of the VPN security arena is huge. It concerns a great deal of data, such that the whole subject is far beyond the focus of this study. What is of concern here is "how do I create a VPN that is relatively secure, monitored, and effectively managed?" There are many vendors who would love to answer that question, some of which include Checkpoint, Cisco, Sonic Wall, and Symantec. This study will focus on the usage of the following products in creating a secure VPN:

- Cisco VPN Concentrator / Client (Link)
- RSA ACE Server (SecurID / RADIUS): (Link)

The following products are included as examples of potential implementation tools. Each of these products could be substituted with a competitor product without significantly altering this example implementation.

- Checkpoint FW-1 4.1/NG (Link)
- Symantec Antivirus (Link)
- Zone Alarm Personal Firewall (Link)
- Microsoft Exchange 2000 (Link)
- Dragon IDS (Link)

The solution described is surely not the only solution available and may not be the best for every network. The goal here is to create an example of a VPN which takes into account several key issues in information security, not to build a VPN that is best for every network. Each network has its own 'personality', fitting its given system uniquely.

II. The Architecture:

Assumptions: The following assumptions are being made:

- The routing between the devices has been preconfigured using Cisco equipment

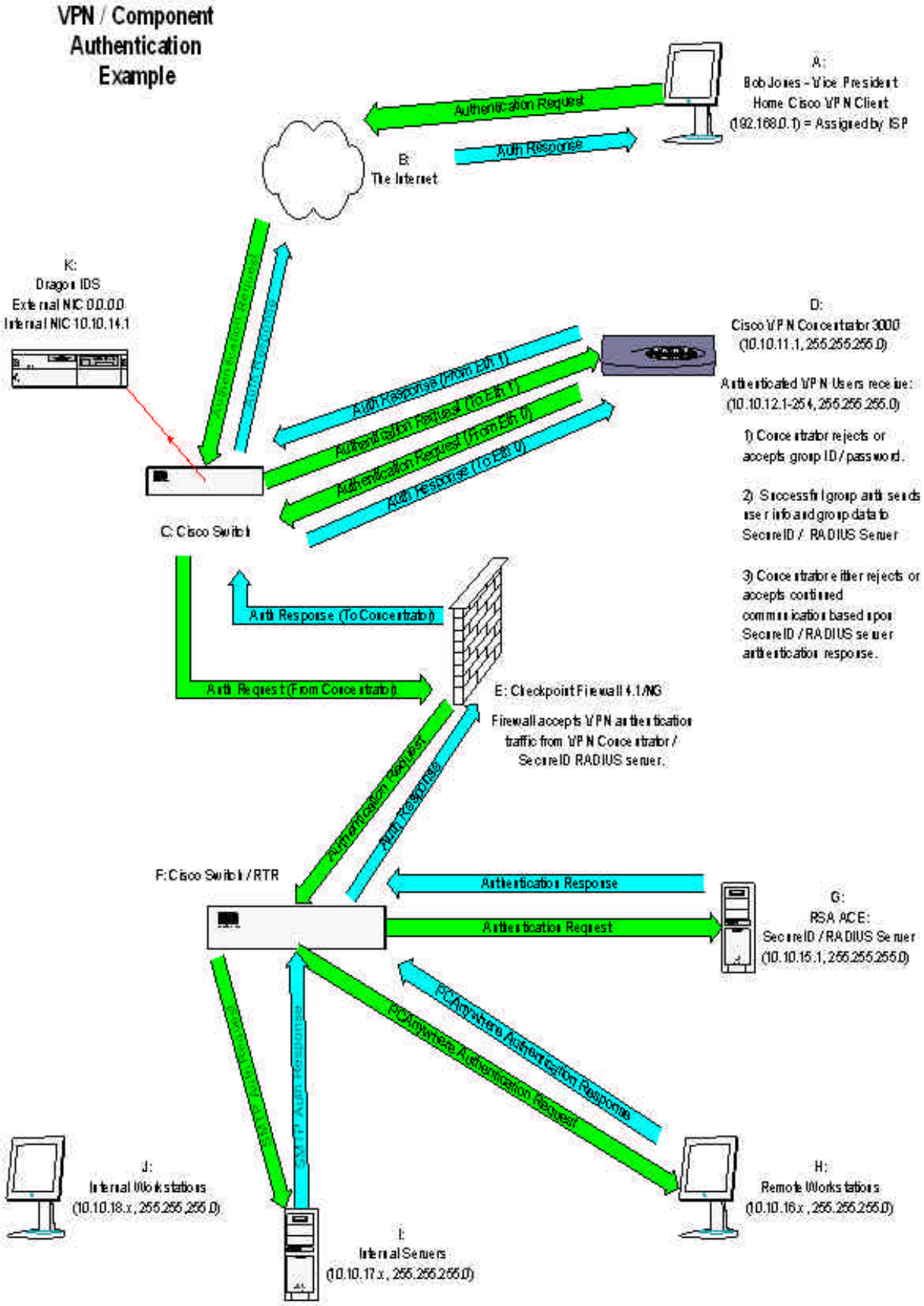
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The internal network is using (generally) a fully patched Windows 2000 architecture
- Although additional steps could be taken to secure the internal network, communication between the internal workstations (J) and internal servers (I) is not limited by any type of filter / firewall. Domain / profile security, however, is implemented. Internal-Remote workstations will have stronger restrictions (H) but are also not limited by filter / firewall. Internal-Remote workstations are not the VPN Clients (A).
- No more than 254 users will be logged in at any given time.
- Some routers have been removed for simplification.

Hardware: The Following Systems are Included in this Diagram

A) Bob Jones Client PC at Home – Bob Attaches via a cable modem and has been assigned the IP address 192.168.0.1 by his ISP
B) The Internet
C) Cisco Switch
D) Cisco VPN Concentrator 3000 (10.10.11.1, 255.255.255.0). Authenticated VPN users receive IP addresses (10.10.12.x, 255.255.255.0), via their RADIUS user ID.
E) Checkpoint Firewall-1 running either 4.1 or NG
F) Cisco Switch
G) RSA / ACE SecurID / RADIUS Server (10.10.15.1, 255.255.255.0).
H) Remote Workstations (10.10.16.x, 255.255.255.0)
I) Internal Servers (10.10.17.x, 255.255.255.0)
J) Internal Workstations (10.10.18.x, 255.255.255.0)
K) Dragon IDS NIDS (External NIC 0.0.0.0, Internal NIC 10.10.14.1) – Sniffs Inbound / Outbound traffic from External NIC in promiscuous mode.

© SANS Institute 2000 - 2002 Author retains full rights.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

Method: The following is a timeline of events for when Bob Jones (A) attaches to the system using his VPN client.

1. Bob presses "connect" on his VPN client login screen and enters his username B%j5o~nn@s and his password. Bob's password is the number listed on his individual PIN number plus the 6 digit number listed on his SecurID token.
2. Bob's communication is routed to the company network via his ISP. Bob's login group uses ESP-3DES-MD5 encryption. This means: Bob's PC is communicating with the company network using a 168 bit Triple DES encryption standard. IPSec traffic uses ESP/MD5/HMAC-128. The IKE tunnel uses 56 bit DES encryption and 128 bit MD5/HMAC authentication. [4] [5]
3. Bob's communications pass through the VPN port (Eth 1) on the VPN Concentrator (D). This port is similar to a firewall in that it "accepts only secure VPN traffic from remote VPN clients" [6] This communication occurs outside of the corporate Checkpoint Firewall (E). All traffic passing through this switch is subsequently 'sniffed' by the Dragon IDS (K). The data 'sniffed' is compared with a database of signatures. If traffic matches a signature, it is logged. In this instance, a VPN signature exists.
4. The VPN Concentrator (D) decrypts the information provided by Bob. The VPN Concentrator authenticates the group ID and password, which are locally stored. If group authentication is successful, Bob's user information is retransmitted to the SecurID RADIUS server (G) at 10.10.15.1. This communication is authenticated by a rule in the firewall. The firewall is configured to accept VPN traffic from the concentrator and the individual clients on a specific interface. (E) Note that the SecurID RADIUS server and the VPN Concentrator are on their own network segments. VPN Concentrator is outside of the FW, SecurID RADIUS server is inside the FW.
5. The SecurID RADIUS (G) piece authenticates the secret key provided by the VPN Concentrator (D). The RADIUS piece then uses SecurID to authenticate the user information sent by Bob Jones.
6. Upon successful authentication of Bob's user data the SecurID RADIUS server (G) sends user profile information to the VPN Concentrator (D). This communication is authenticated by a firewall rule (E). From the profile data the VPN Concentrator (D) sends a static IP address and DNS

---

[4] *Cisco VPN 3000 Concentrator Documentation.* Feb 11th 2002
http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/3_1/admin/vcach1.htm

[5] *Users Manual for Cisco VPN Concentrator: IPSec SA. 2000*

[6] *Installing and Cabling the Chassis (Cisco Concentrator 3000).* Mar 19th 2001
http://www.cisco.com/univercd/cc/td/doc/product/aggr/vpn5000/5000hw/5001hw/install/install.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

settings to Bob's VPN client. This data was provided by the SecurID RADIUS server (G).

7. Bob's VPN client is assigned the IP address 10.10.12.1 by his RADIUS user profile. Other users are assigned addresses between 10.10.12.2 and 10.10.12.254.
8. Bob has now established a SecureVPN tunnel to the corporate network. Although it is possible to enable direct mapping of drives within his corporate domain, Bob's company has chosen not to enable that option for him, due to security concerns. If Bob's PC were to be hacked, easy access could be given to major network resources. Instead, via firewall regulation, Bob only allowed SMTP traffic between his VPN client and the company email sever (I) and also PCAnywhere traffic between his VPN client and the company remote workstations (H). Each of these is on separate network segments, as is depicted in the diagram.
9. When Bob logs into a remote workstation via PCAnywhere the login is subsequently recorded, as is all other communication in the process. These logs are reviewed by IS Security personnel.
10. Through the remote workstation which he attached to via PCAnywhere, Bob logs into the corporate domain. He now has access rights associated with his domain profile and can work as though sitting at his desk.
11. All the time while he is working Bob has a personal firewall (Zone Alarm) and antivirus (Norton Antivirus Corporate Edition 7.6) active. Currently, Bob's computer is one of the weakest points in the network. He is protecting himself and the network using these tools, in addition to the login methods described. If Zone Alarm were to be deactivated, the VPN Concentrator would drop the connection, as a setting has been selected which disallows connections without a personal firewall present. This helps to filter out negligent employees who user their VPN without caring about the security of their home computer.

III. Implementation:

Cisco VPN Concentrator 3000

The beginning of this overview discussion will be the Cisco VPN Concentrator 3000. Instead of using a software solution provided by Microsoft, or the Secure VPN Checkpoint product, Bob's company has selected the Cisco VPN 3000. This is because:

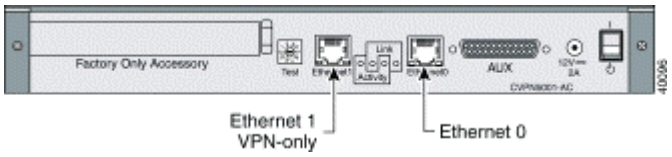
- It is totally separate from the FW causing no performance hit against the FW itself, except due to the rules created to allow the VPN devices to communicate with the internal network.
- It is compatible with the Cisco environment already running.
- It offers multiple means of configuring including telnet and web based.
- It offers a detailed logging mechanism

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- It integrates well with various authentication, accounting, DNS, DHCP, and NTP servers.

Setup will proceed as follows.

1. Use the following diagram:



[7]

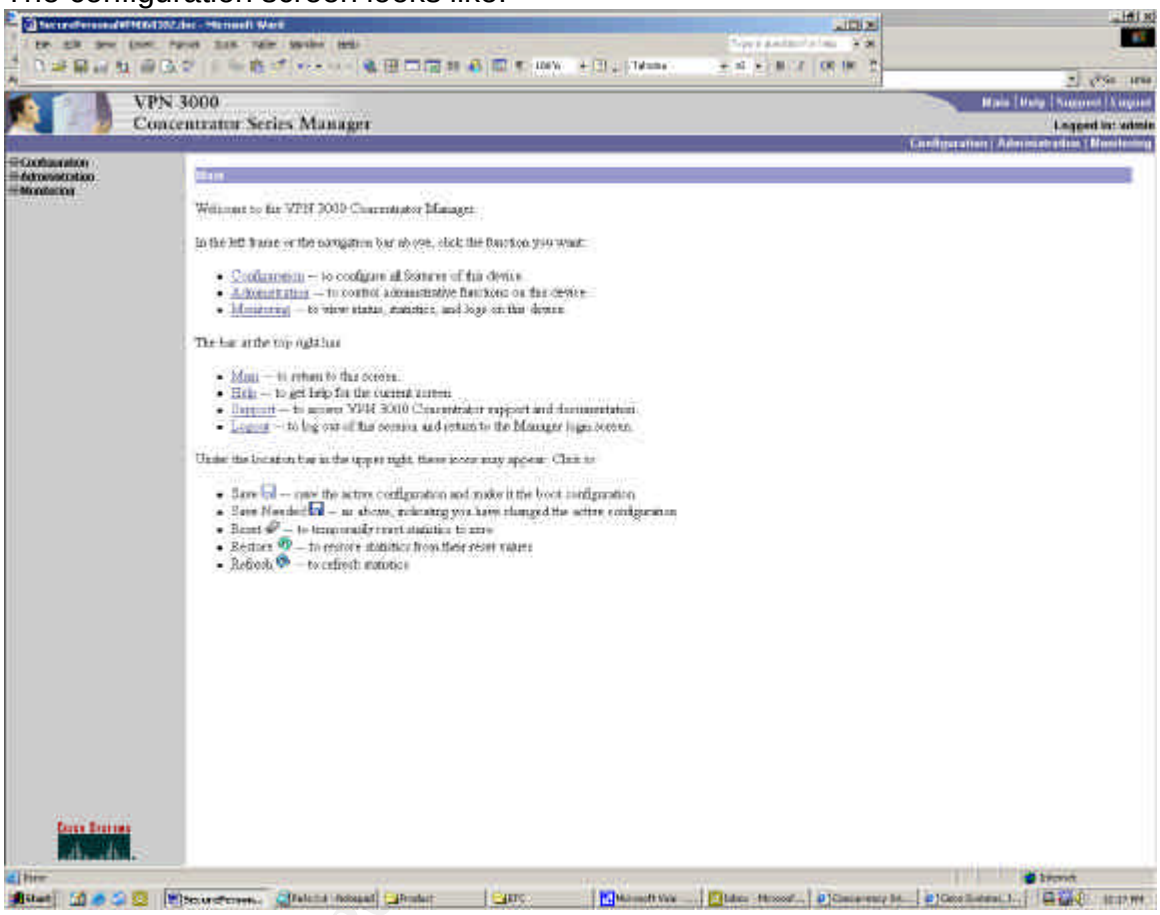
   a. Attach Eth 1 to the external segment on the Cisco Switch (C).
   b. Attach Eth 0 to the internal VPN segment on the Cisco Switch (C). Communication will be forwarded from the switch, through the firewall, to the SecurID RADIUS server.

2. Attach a serial cable to the VPN Concentrator and boot the system for the first time. Use the following settings: (All of these options can be changed later.)
   a. Password for admin account
   b. Time Zone / DST
   c. Externally addressable public address for Eth 1.
   d. Internal address of 10.10.11.1 for Eth 0.
   e. System name
   f. DNS
   g. Default Gateway
   h. Enable PPTP, L2TP, and IPSec.
3. Create a rule in the firewall which allows web communication between your administration PC and the VPN Concentrator Eth 0 address. To be more secure, setup your VPN administration PC as 10.10.11.2 on the 10.10.11.x segment.
4. From the administration PC access the VPN Concentrator console through a web browser. Login using the administrator account.

[7] *Installing and Cabling the Chassis (Cisco Concentrator 3000).* Mar 19th 2001 http://www.cisco.com/univercd/cc/td/doc/product/aggr/vpn5000/5000hw/5001hw/install/install.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5. The configuration screen looks like:



6. Setup NTP
    a. Configuration => System => NTP => Hosts, Parameters
7. Enable / Disable Configuration Management Protocols
    a. Configuration => System => Management Protocols.
        i. Enable HTTP / HTTPS to use web access
        ii. Enable Telnet to use serial, network command line access
        iii. Enable TFTP to send new IOS patches to the Concentrator 3000.

8. Configure Address Management
    a. Configuration => System => Address Management => Assignment
        i. Check “use address from authentication server” and “use address pools”. These choices are used in order of decent. The Concentrator will grab an address from the RADIUS server first. The address pools exist in case the profiles fail to give a client an IP address.
        ii. In “Pools” create a pool entry for the network 10.10.13.0, 255.255.255.0. The pooled addresses are on a different segment since addresses in the 10.10.12.0 segment are

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

assigned by profiles and receive specific access rights by the firewall. The pooled addresses may need to be managed differently if they are assigned in this manner, such that access over the 10.10.12.0 segment would be generic and would only be allowed very reduced access. Alternatively, backup pools could be removed completely, simply accepting that if for some reason a person is not assigned an IP address by the ACE Server VPN Access will be denied.

9. Configure Groups
    a. Configuration => User Management => Groups
        i. Create a group called VPN1 and enter into the settings modification.
            1. Identity
                a. Enter a group password. The group password should be a strong password, using special characters, numbers, and letters. Try not to use combinations of words.
                b. Type = Internal. Setting the type to internal means that the group itself is configured only on the VPN Concentrator. Groups can also be setup on RADIUS servers and such, but in this example we are only setting up users on the RADIUS server.
            2. General
                a. Set primary DNS and primary WINS to the internal server addresses. These addresses are given to authenticated VPN clients.
            3. IPSec
                a. Set the IPSec SA to ESP-3DES-MD5
                b. Select authentication RADIUS
            4. Mode Config
                a. Create a banner which is displayed upon client login to the VPN system. This banner is used to inform the VPN client as to the terms of use.
                b. If some clients are using personal firewalls at home you may need to enable IPSec over UDP.
            5. Client Firewall
                a. Enable this setting in conjunction with a personal firewall of choice, be it the Zone Alarm personal firewall or the Cisco Client Firewall.
            6. HW Client

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

a. Select Require Interactive Hardware Client Authentication. This setting demands that the VPN Client PC be authenticated.
b. To simplify the example, do not select that the individual user behind the authenticated VPN Client PC be authenticated.

ii. Modify Auth Servers => Add
1. Select Server Type = RADIUS
2. Authentication Server = 10.10.15.1 (Address of SecurID RADIUS Server)
3. Server Port = 1645
4. Set the RADIUS secret password. Use a 'strong' password.

10. Configure Default Gateways
a. Configuration => System => IP Routing => Default Gateways
i. Select Default Gateway – This address will conform to the external LAN interface on the default router.
ii. Tunnel Default Gateway – This address will conform to an interface on our Checkpoint Firewall. [8]
11. Configure Static Routes
a. Configuration => System => IP Routing => Static Routes
i. Create a default route to send all external traffic to the Default Gateway address.
ii. Create routes to the internal network which conform to the Tunnel Default Gateway.

RSA SecurID RADIUS Server:

The SecurID RADIUS server provides two-factor user authentication which is far more secure than the standard single password challenge-response. Users are given a SecurID token which contains a hashed number synchronized with Greenwich-Meantime. This number can be of various lengths. When authenticating, a user enters both their user name and their password. The password is made up of a unique pin number and the number shown on the SecurID token.

The RADIUS piece allows for users to receive specific information, such as an IP address and subnet assignment, in their user profiles. This enables accountability for VPN communications.

As shown in the diagram, the SecurID RADIUS server lies behind the firewall, such that the firewall must be configured to allow for the two servers to communicate. A rule should be added to the Checkpoint FW as follows:

[8] *Users Manual for Cisco VPN Concentrator: ###.###.###/help/ip.html#defroute*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

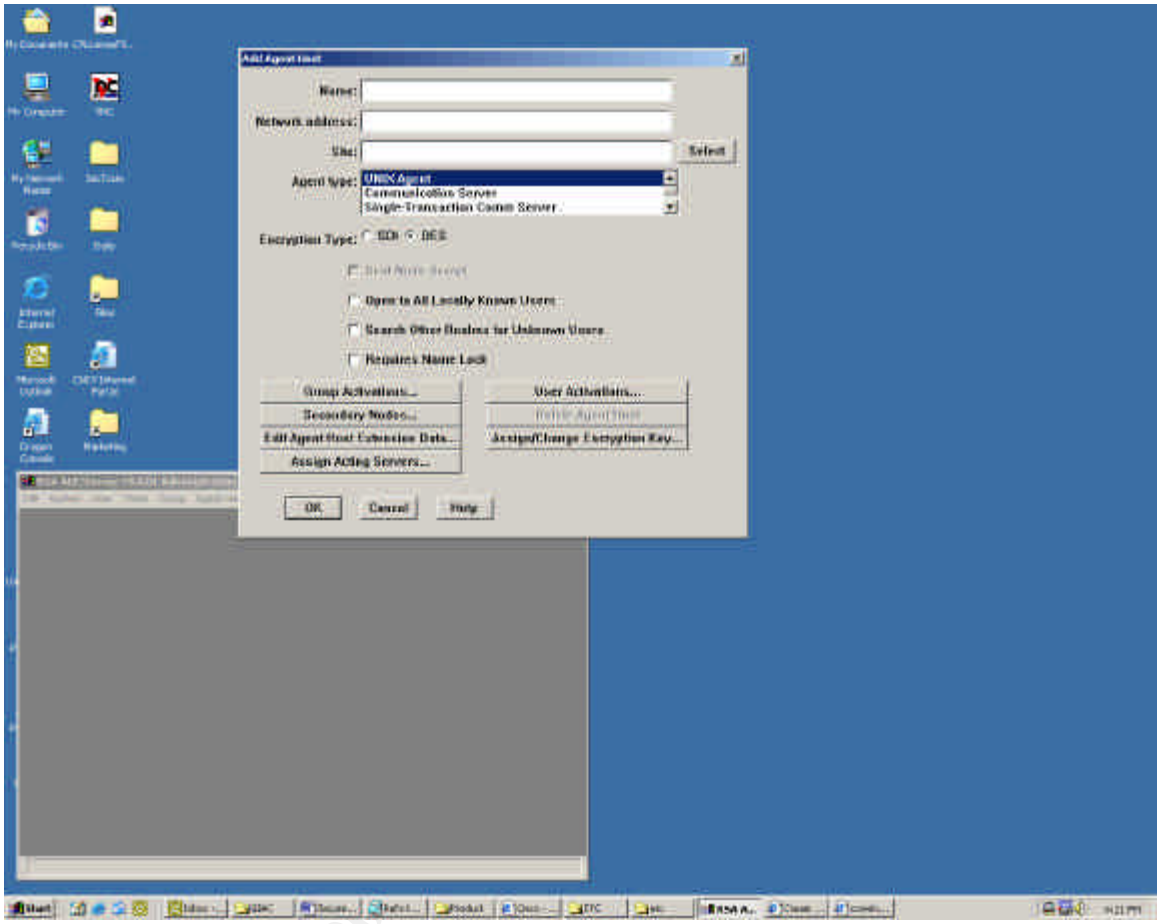
Rule 1:
From: 10.10.11.1 (VPN Concentrator) or 10.10.15.1 (SecurID RADIUS server)
To: 10.10.15.1 (SecurID RADIUS server) or 10.10.15.1 (VPN Concentrator)
Service: RADIUS
Action: Accept
Track: Account
Time: Any

Setup will proceed as follows:

1. Hardware Setup
    a. Build a clean and updated Windows 2000 server.
    b. Situate the server and any replica servers on a unique segment. (10.10.15.0, 255.255.255.0) In this instance the ACE Server has been designated 10.10.15.1.
2. Installation / Prep
    a. Begin ACE server setup program. Follow the installation instructions for installing a new **Primary ACE/server**. [9]
    b. In the file %systemroot%\system32\drivers\etc\services add the following services:
        i. Radius = 1645/udp
        ii. Radacct = 1646/udp (Note: These ports vary. Check with the software version being installed.)
    c. In the 'Configuration Management Console' ensure that the following settings are accurate:
        i. Encryption Type = DES
        ii. RADIUS Server Enabled = Checked
        iii. RADIUS = same port as in services file.
        iv. In 'Agent Host' configure incorrect login information for hosts.
3. Database Administration Console Setup
    a. Open the Database Administration Console.
    b. Add the VPN Concentrator:

[9] *RSA ACE/Server 5.0 for Windows NT and Windows 2000: Installation Guide*. p25-39 June 2001.

© SANS Institute 2000 - 2002, Author retains full rights.

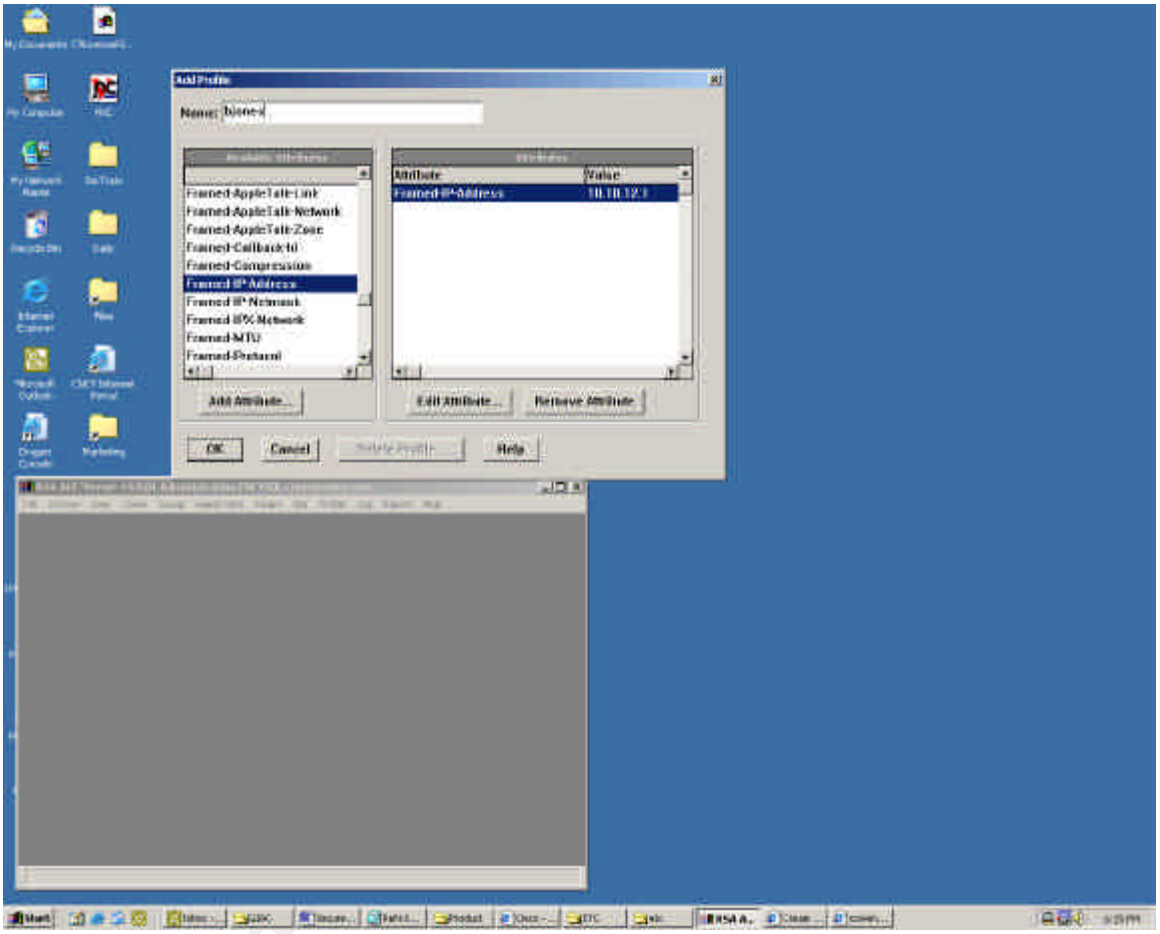


i. Agent Host => Add Agent Host
ii. Name = VPNConcentrator1
iii. IP = 10.10.11.1
iv. Agent Type = Communications Server
v. Encryption Type = DES
vi. If all created users will be given access through the VPN concentrator select “open to all locally known users”. Else, leave this field blank.
vii. Assign your ACE server as the “Acting Server”.
viii. Add the RADIUS secret password under “Assign / Change Encryption Key”. This password must be the same as the one entered into the VPN Concentrator group. If it is not the same communications will not be possible.

c. Import Tokens:
   i. Tokens => Import Tokens => Select Token File that was included with Key Fobs.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

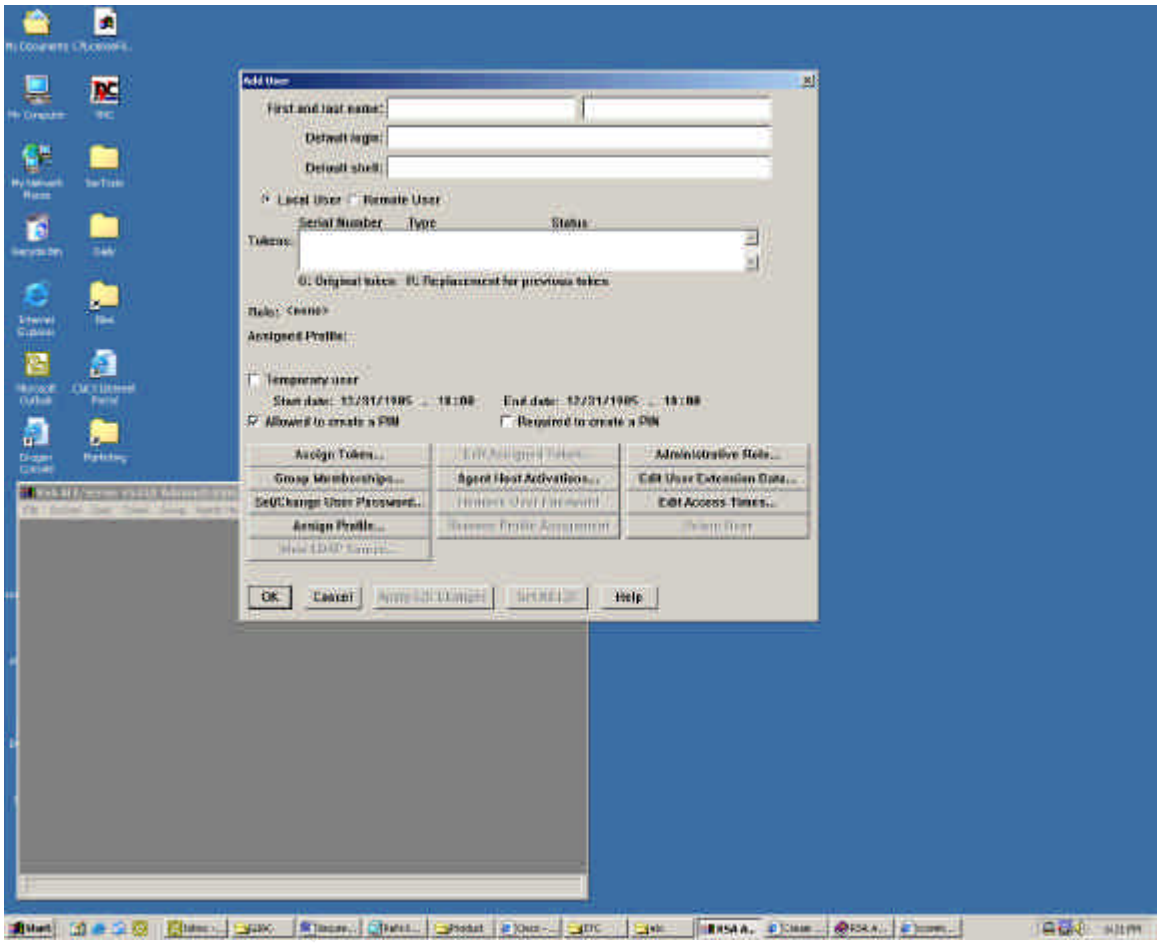
d. Create Profile



i. Profiles => Add Profile
ii. Name = bjones
iii. Attribute = Framed IP Address = 10.10.12.1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

e. Create Users: (User Creation Console)



i. User => Add User
ii. Enter First and Last Name
iii. Create a strong default login. Strong logins are yet another security precaution that can be taken. Even if a hacker had Bob's unique PIN and token he would still have problems gaining access since the user-name is not known. Ex: Do not create user bjones for Bob Jones. An example of a strong user-name is "B%j5o~nn@s".
iv. Assign a Token (Key Fob) through "Assign Token". The first login will ask Bob to select a unique PIN. This can be done either by logging into the VPN or by IS staff doing a pre-test via a remote RADIUS authentication client. If IS staff creates a PIN for Bob he will need to commit it to memory, rather than write it down. Bob should be prevented from selecting a PIN number like his birthday or anniversary. PINs like this are very easy to guess.
v. Assign Bob the profile bjones.

© SANS Institute

vi. If "open to all locally known users" is not known on all required agent hosts, then activate the user through "Agent Host Activations" on those hosts that the user is not active.[10]

4. Firewall Rules – Bob needs to have firewall rules setup to manage his access rights when connected to the network via VPN. Bob has authority to do the following:
   a. Retrieve SMTP mail from corporate Exchange 2000 server. (Another SMTP server would be relevant as well.) Configure a firewall rule as follows:

      1. Source = 'Exchange Server' – 10.10.17.1 or 'VPN-Users-SMTP'. Bob is a member of the 'VPN-Users-SMTP' group.
      2. Destination = VPN-Users-SMTP' or 'Exchange Server'
      3. Service = SMTP
      4. Action = Accept
      5. Track = Account
      6. Time = Any (Unless access times are regulated.)

   b. Attach to a PCAnywhere host in the Remote Workstations segment. (H) Configure the firewall rule as follows:

      1. Source = 'Remote-Workstation-Net' – 10.10.16.x or 'VPN-Users-Remote'. Bob is a member of the 'VPN-Users-Remote' group.
      2. Destination = 'VPN-Users-Remote' or 'Exchange Server'
      3. Service = PCAnywhere
      4. Action = Accept
      5. Track = Account
      6. Time = Any (Unless access times are regulated.)

Dragon:

Enterasys Dragon is an Intrusion Detection System (IDS) which is not unlike many snort derivatives. This overview will not discuss the particulars of implementing Dragon IDS itself, though it will discuss the creation of a VPN signature, as well as placement.

With this implementation, Dragon IDS should be setup on a machine with two NICs. One which is situated on the external segment assigned the IP address 0.0.0.0. This address hides the sensor from the outside world. The monitored segment needs to be set to 0.0.0.0/32, which allows the sensor to sniff all data

[10] *Configuring VPN 3000 Client to Concentrator with IPSec SDI* Authentication. Feb 07, 2002 http://www.cisco.com/warp/public/471/sdi.html

© SANS Institute 2000 - 2002 Author retains full rights.

coming across the line. In this example, the second NIC will be given the IP 10.10.14.1. In this case, the firewall needs to be configured for the following:

1. Source = Dragon Sensor (10.10.14.1) or Dragon Server (10.10.17.3)
2. Destination = Dragon Server (10.10.17.3) or Dragon Sensor (10.10.14.1)
3. Service = TCP Port 9111 and TCP Port 9112
4. Action = Accept
5. Track = Log
6. Time = Any

There are various ways to create signatures to monitor VPN:

1. Report on traffic on the UDP or TCP port through which the concentrator and client communicate. This will be either 500/UDP, 10000/UDP, or 10000/TCP.
2. Report on all traffic coming or leaving the external IP address of the concentrator.
3. Use ethereal to capture data to and from a VPN client. Use that data to create a unique signature for your VPN traffic.

Other Uses for Snort Derivatives:

1. Monitor PCAnywhere traffic from an authenticated client (Bob – 10.10.12.1) to a Remote Workstation.
2. Monitor SMTP traffic from an authenticated client (Bob – 10.10.12.1) to the internal SMTP server.

Client Side Firewall and Antivirus:

An important piece of the Secure VPN architecture is client side protection. When connected to a VPN the client becomes the “weakest link” in the network because these computers are often home PCs with the VPN Client installed on them. Unfortunately, hackers have figured out that it is often fairly easy to compromise a home VPN Client. That client can be used to gain significant access to the internal corporate network. Also, attacks hidden within an authorized user’s login can be harder to detect. It is easier to see an attacker attempting to exploit an IIS 4.0/5.0 vulnerability than it is to see a Trojan slip through a VPN tunnel into a internal network workstation. These worms can be spread to clients via a variety of methods, some of which include personal email, attaching to infected web-sites, using file swapping clients like Kazaa and Morpheous, and diskette sharing. Many of these are a derivative of shared home use, such that a PC becomes both a work PC and a home PC.

Generally it is a better idea to have a dedicated PC for VPN Client access, but that is not always the case. In most cases, not only is this PC used for work, but also for family use. This situates the PC on a delicate security teeter-totter. One

© SANS Institute 2000 - 2002, Author retains full rights.

of the better ways to deal with this is to have adequate client protection programs installed, like a Client Side Firewall and Antivirus.

An example of a Client Side Firewall is Zone Alarm. Personal firewalls are not substitutes for corporate firewalls, but they do provide adequate protection to single PCs operating in a home or VPN client environment. Zone Alarm itself is fairly customizable. Upon installation of the program the user is prompted for each particular external access attempt. Users are asked if a particular access should be allowed or denied. In a corporate environment, these rules can be pre-set so that the user is required to have a particular rule-set in order to attach to the VPN.

Zone Alarm has further partnered with Cisco to develop a product that integrates completely with the Cisco 3000 series Concentrator. [11] As discussed in the VPN Concentrator setup, Zone Alarm and other personal firewalls can be enabled as required components of VPN authentication, such that a client will not be allowed access if a personal firewall is not active.

So how secure is the personal firewall? It is certainly not as robust or as inclusive as the dedicated solutions provided by Checkpoint and Cisco, though it does provide a modest amount of protection. The hope is that the protections provided by Zone Alarm or another personal firewall will denture an attacker and possibly make them direct their activities elsewhere.

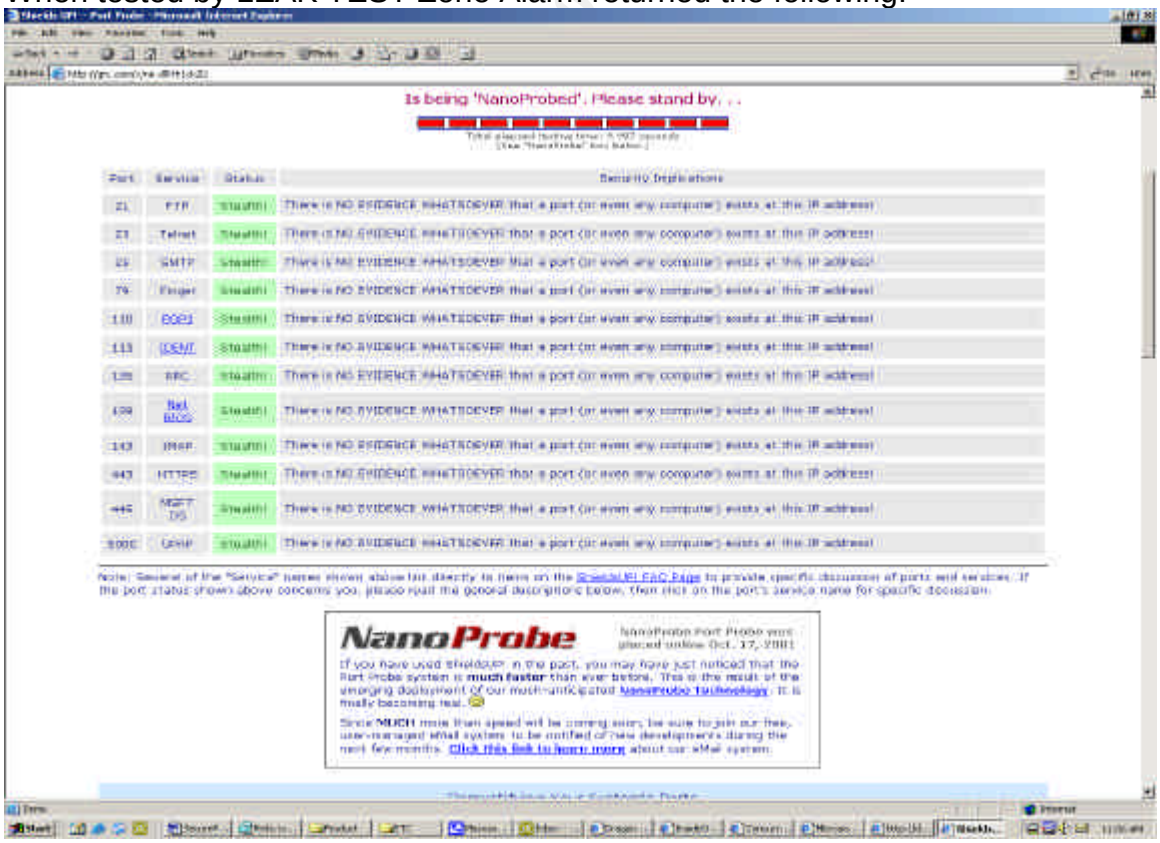
Although it is certainly not inclusive, testing at GRC.com returned the following results:

[11] *Cisco VPN 3000 Concentrator Series* Integration. Zonelabs, 2002. http://download.zonelabs.com/bin/media/pdf/Int_Ciscovpn_FINAL.pdf

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

When tested by SHIELDS UP Zone Alarm returned the following:

When tested by LEAK TEST Zone Alarm returned the following:



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The results provided by GRC.com indicate that Zone Alarm is providing at least some level of protection against intruders.

Zone Alarm and Cisco have also partnered with antivirus firms such as Symantec and McAfee, which provide protection against various types of worms and viruses that spread rampantly across the internet. Since many users check email outside of their corporate account there may be the possibility that a user will receive an infected email without passing through the corporate SMTP antivirus scanners. With a client-side antivirus implemented this contingency is accounted for and can usually adequately protect against most viruses. Having an antivirus work in conjunction with a personal firewall significantly improves the base security of a VPN Client.

IV. Management:

Far too often, IT professionals stop caring about their systems after the technical environment is in place. Only once something noticeably breaks, do they look at their systems. However, the implementation of proper system management is key to maintaining a secure system.

The implementation of policies and procedures can significantly enable the strength of corporate security, especially in regards to VPN usage.

Policies:

What is a policy? A policy defines the “who, what, where, when, and how” of an organization. It defines exactly what the regulations and requirements are within the organization. Implementing strict policies not only keeps the users in-line, but also aids in enforcement. When usage is given in writing and outlined in person a user can understand exactly why they have certain access privileges and why they do not. The absence of policy can lead to both an inability to manage the access of particular users and also the inability to enforce any kind of restrictions.

The following requirements should be considered in a VPN security policy:

Who: Each company must determine exactly who can and cannot have access to the VPN? Does accounting intern Steve really need access or can he drive 10 minutes to work? Considering the difference between who wants access and who needs access is a critical factor in maintaining a secure infrastructure.

What: What are the users attaching to the VPN to do? What do they want to do and what do they need to do? Similar to what users get access, someone also has to determine what type of access that user receives.

© SANS Institute 2000 - 2002, Author retains full rights.

Where: From where can a user attach to the VPN? Can the user connect with their home PC or do they need to use a dedicated corporate laptop / workstation? Determining the answers to these questions will significantly alter the environment required to maintain VPN security. Dedicated corporate laptops will certainly be more manageable and securable than the home PC employee X brought home from Best Buy.

When: When can specific employees attach to the VPN? Do they have access requirements or limits? Sometimes it is prudent to only allow specific employees access during certain times of the day / night. Enforcing this type of policy will improve accountability.

How: Through what manner will a user attach? What level of encryption? Do they need to have both an antivirus and a personal firewall running?

Procedures:

What is a procedure? A procedure is a system activity that needs to be repeated on a regular basis. Procedures can be used to plan, build, implement, and test a system. They can also be used to react to situations. Implementing regularly performed procedures is critical to system monitoring. An employee needs to confirm that the defined access policies are also being enforced. For example: Employee Y is assigned the task of monitoring the Concentrator and SecurID/RADIUS server logs for inconsistencies. Employee Y is assigned the task to perform that procedure four times daily. This becomes not only a way to monitor VPN usage, but is also an employee management tool.

Monitoring the VPN network activity is critical to maintaining the security of the network. The purpose of logging activity is not simply so that large issues can be resolved; it is also so that small issues do not become large issues. Logging also adds accountability to user action since every data transfer initiated over the VPN is recorded by a logging system. The logging systems included are (in order of appearance):

1. Dragon IDS logging
2. Cisco VPN Concentrator
3. Checkpoint Firewall
4. SecurID/RADIUS Server
5. SMTP Email Server
6. Remote Workstations

The monitoring personal should verify that (1) all authorized communications are occurring successfully and (2) all unauthorized communications are being prevented and reported upon.

V. Conclusion:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Although the VPN has provided the corporate community with significant advantages in terms of off-site productivity, it has also created several very complex security issues. The implementation of security and accountability controls is critical to a sound VPN management. Those controls need to be implemented by way of well planned network infrastructure and adequate policy / procedure management.

The infrastructure presented in the VPN Concentrator / SecurID RADIUS implementation presents just one method of creating a secure VPN setup. There are many products and tools which are also effective in accomplishing the same goals, such that networks are very unique. A VPN implementation should be consistent with the 'personality' of the network, and should not be implemented in a "one-size-fits-all" fashion.

Adequate policies and procedures need to be implemented to maintain and manage the VPN infrastructure and users. Without the policies and procedures to back it up an infrastructure means nothing.

Lastly, a VPN system must be completely tested before and during its implementation. It is difficult, if not impossible to confirm system security and integrity without regular testing. Testing and monitoring changes via system logs, sniffers, and network scanners enables the security professional to better secure the corporate network. A good security professional will learn that security is a dynamic process, one that is never complete and is always changing.

© SANS Institute 2000 - 2002 Author retains full rights.

Reference:

Cowell, Ruth. *War Dialing and War Driving: An Overview,* June 11th, 2001
http://rr.sans.org/wireless/war.php

Webopedia Article. *T-1 Carrier,* January 9th, 2002
http://www.webopedia.com/TERM/T/T_1_carrier.html

Webopedia Article. *T-3 Carrier,* February 8th, 2002
http://www.webopedia.com/TERM/T/T_3_carrier.html

Cisco VPN 3000 Concentrator Documentation. Feb 11th 2002
http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/3_1/admin/vcach1.htm

Users Manual for Cisco VPN Concentrator: IPSec SA. 2000

Installing and Cabling the Chassis (Cisco Concentrator 3000). Mar 19th 2001
http://www.cisco.com/univercd/cc/td/doc/product/aggr/vpn5000/5000hw/5001hw/install/install.htm

Installing and Cabling the Chassis (Cisco Concentrator 3000). Mar 19th 2001
http://www.cisco.com/univercd/cc/td/doc/product/aggr/vpn5000/5000hw/5001hw/install/install.htm

Users Manual for Cisco VPN Concentrator: ###.###.###/help/ip.html#defroute[1]

RSA ACE/Server 5.0 for Windows NT and Windows 2000: Installation Guide. p25-39 June 2001. [1]

Configuring VPN 3000 Client to Concentrator with IPSec SDI Authentication. Feb 07, 2002
http://www.cisco.com/warp/public/471/sdi.html

Cisco VPN 3000 Concentrator Series Integration. Zonelabs, 2002.
http://download.zonelabs.com/bin/media/pdf/Int_Ciscovpn_FINAL.pdf

© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: July 23rd, 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 New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 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
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
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 Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	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 Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
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
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