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

SANS Institute
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4

Authenticating Nortel Contivity Clients using RSA SecurID Tokens
Rusty Fancher
June 18, 2002

Introduction

Today, more and more companies are using VPN Technology. It allows their professionals to access sensitive company information more conveniently. The challenge is to provide a higher level of protection than just a user name and memorized password. But how do you ensure confidentiality? How do you ensure it is your professionals connecting and not an intruder? If a hacker can determine the client configuration and a valid user ID and password, then the system will be compromised no matter how much effort you put into the rest of the VPN architecture.[1] The optimum solution is a VPN using 3DES Encryption with Strong Authentication.

Nortel's line of Contivity Secure IP Services Gateways, also known as the Contivity Extranet Switch (CES), coupled with RSA ACE Server using SecurID for Strong Authentication provides an excellent solution. With this configuration, your design can be bathed in security features. By assigning profiles on the RSA ACE Server, you provide both Authentication and Authorization. The Contivity can make use of Interface Filtering, an optional Secure Stateful Firewall, or a Check Point Firewall-1 server for added authorization. A custom Nortel VPN Client package can be created for a password protected, automated installation. This Extranet solution will prevent your advanced users from tinkering with their setting; as well as, ensuring that your least technical person can still use it.

Choosing a VPN

With all the VPN solutions around, why use Nortel's Contivity Gateway?

> As a market leader in IP Virtual Private Networking (IP VPN), Contivity has been delivering secure end-to-end IP VPNs for years. Contivity VPN capabilities are standard in every unit. and include support for standard IPsec tunneling, authentication and encryption services. Contivity also offers broad support for all leading digital certificates (PKI), strong authentication, global dialer, personal firewall, intrusion detection and directory vendors to ensure customers can deploy best-of-breed end-to-end solutions. Contivity has been certified by both TruSecure

[1] THUR

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

(ICSA) for IPSec multi-vendor interoperability, and by the Federal Government's FIPS-140 certification process to ensure high levels of security compliance [2]

Well, enough of the "Marketing Fluff", as I like to call it. Let's get to the real reasons why the Contivity provides you with an excellent foundation for building a secure remote access solution. In 2001, Gartner Dataquest ranked Nortel as the number one producer of global telecommunications equipment.[3] The biggest reasons for its success are flexibility, scalability and security. The Contivity can be configured in a million and one different ways. It can be used to create both User Tunnels and Branch Tunnels (LAN to LAN). Unfortunately, all the different tunnel configurations are beyond the scope of this document.

In this document, we will focus on securing an IPSec User Tunnel with Two-Factor Authentication. IPSEC technology is based on modern cryptographic technologies, making possible very strong data authentication and privacy guarantees.[4] The Contivity can be either placed behind your Internet Firewall in a DMZ or in parallel (see figure 1 below). For ease of configuration, we will focus on running the Contivity in parallel to the Internet Firewall.

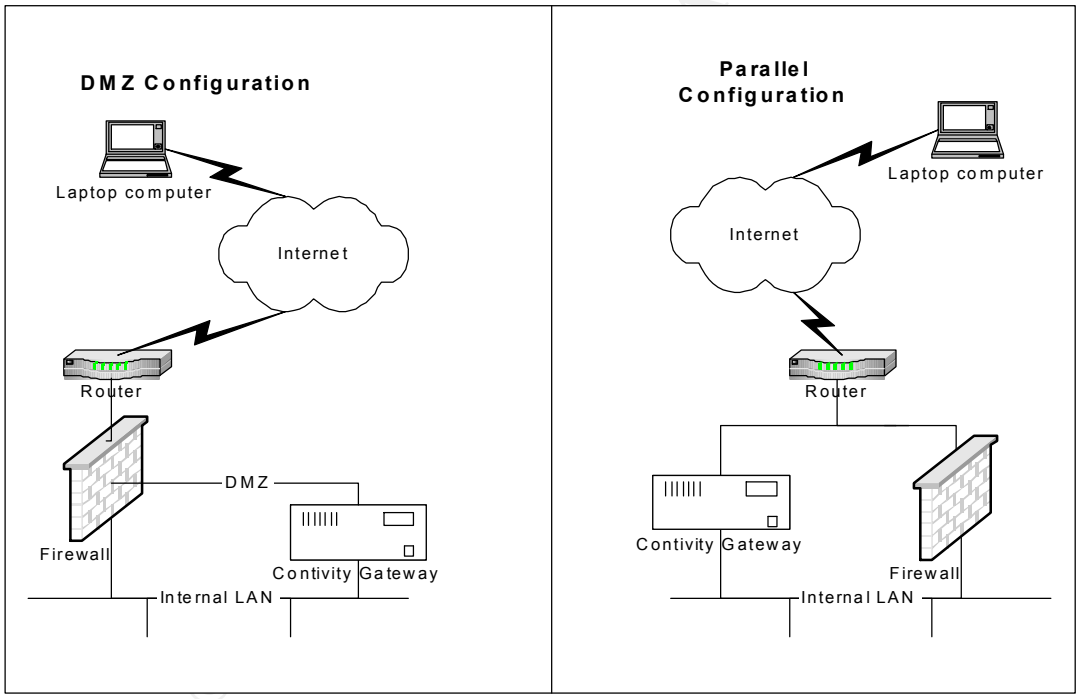


Figure 1. DMZ and Parallel implementation of Contivity

[2] NORT1
[3] FVPN
[4] NICH

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

Choosing a Authentication Method

What is Strong Authentication and why do I need it? Strong Authentication is a measure designed to verify an individual's authorization by presenting two or more items. Probably the best example of Strong Authentication is using your bank's ATM to access your account. It requires that you have your ATM Card (something you have) and your personal PIN (something you know) before you can access your account. Two-factor authentication provides a higher level of trust than passwords alone because it requires something a user knows, such as a password, as well as something that person has, such as a smart card or a token.[5] How safe would you feel if someone could just walk up, stick in your bankcard, and have complete access to your account? Now think about your company's sensitive information. It just makes sense to protect that data with the same level of security as you do your money.

Through the RSA SecurID Ready Program, the products of more than 140 leading vendors of firewalls, remote access servers, VPNs and Web applications support RSA SecurID two-factor authentication right out of the box.[6] The SecurID Token is more secure than just a simple password, but it provides you the same ease of use as a simple password. A new one time use password is created every 60 seconds providing you with a virtually hack proof authentication method. After securing your VPN solution, you can begin securing other resources too. Therefore, you can maximize your Return On Investment (ROI).

The ACE Server allows you to assign your users to groups. These groups can be used to authorize where your users are allow to authenticate. You can also assign profiles in the ACE Server Database. The profiles can be used to push RADIUS Attributes to the Contivity. Once authenticated, the CES receives the RADIUS Attributes and then uses them to pull configuration settings from the appropriate Group configured on the Contivity. The settings are then applied to the Contivity Extranet Client. I will discuss the benefits of using this method of authorization and authentication a little later in this document.

Implementation Requirements

There are a few requirements to implement a successful solution. The Contivity Extranet Switch must be a CES 4000, CES 2000 or CES 1000 series model. Below are a few of the key features to help you decide which model fits your needs:

Contivity 1700	Contivity 2700	Contivity 4600
Memory: Standard – 128MB Maximum – 256MB	Memory: Standard – 128MB Maximum – 256MB	Memory: Standard – 256MB Maximum – 1 Gigabyte
850 MHz processor	1.33 GHz processor	Dual 800 MHz

[5] [HULME]
[6] [RSA1]

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

		processors
1 PCI Expansion Slot	3 PCI Expansion Slots	5 PCI Expansion Slots
LAN/WAN Interfaces: Standard - 2 10/100 Base-T Ethernet - Management/Console (DB-9) Optional - Additional 10/100 Base-T - Single-Port V.35/X.21 - T1 with integrated CSU/DSU	LAN/WAN Interfaces: Standard - 2 10/100 Base-T Ethernet - Management/Console (DB-9) Optional - Additional 10/100 Base-T - Single-Port V.35/X.21 - T1 with integrated CSU/DSU - High Speed Serial Interface (HSSI)	LAN/WAN Interfaces: Standard - 2 10/100 Base-T Ethernet - Management/Console (DB-9) Optional - Additional 10/100 Base-T - Single-Port V.35/X.21 - T1 with integrated CSU/DSU - High Speed Serial Interface (HSSI)
Up to 500 tunnels*	Up to 2000 tunnels*	Up to 5000 tunnels

** Note: Contivity 1700 comes with 200 VPN Tunnel License and Contivity 2700 comes with 1000 VPN Tunnel License. An upgrade can be purchased to add additional VPN Tunnel Licenses*

A complete feature list of the Contivity Switches can be found in document 55129.02-04-02.pdf:

http://www.nortelnetworks.com/products/library/collateral/55129.02-04-02.pdf[7]

The CES must be running software version 2.0 or higher. The latest release currently available is version 4.06. The ACE Server should be version 4.1 or higher due to the fact it has built in support for RADIUS. The latest version for the ACE Server is 5.02. Several models of SecurID Tokens can be utilized. Models SD200, SD520, and SD600 are available. The most popular model is the SD600 SecurID Token or FOB.

Assumptions made by this paper:

This paper is written with several assumptions being made because they are outside the scope of this paper. First assumption is that you have your Contivity setup correctly for your environment and you can authenticate to the Internal LDAP database using the CES Client. This configuration will also have the appropriate filters defined and firewall features enabled. Second assumption is that your ACE Server, running on Windows NT or 2000 server, is also setup correctly for your environment. At a minimum you should be able to authenticate to the server locally using your SecurID Token. The ACE Server must be licensed for RADIUS Support and have the RADIUS Services running on Port 1645. The final assumption is that you have network connectivity between the

[7] [NORT2]

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

two devices. I would also suggest that you do not have any filtering between these two devices until after everything has been setup and tested. Then you can go back and add filtering rules as necessary to meet your security needs. This paper will also only focus on the options that must be set to allow your Contivity to communicate with the ACE Server using the RADIUS protocol for Two-Factor Authentication.

Contivity Configuration Changes

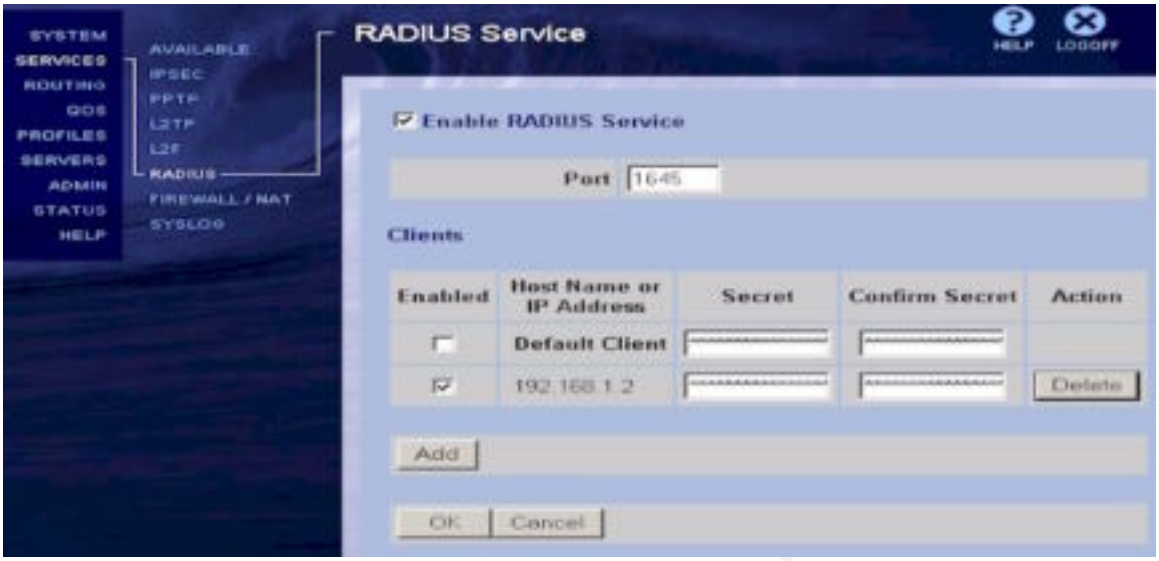
You will need a computer that has the ability to browse to the Management Interface of the Contivity. After logging into the Management Interface, you will have access to the Web based graphical user interface for managing the Contivity. Then you can follow the steps below to complete the necessary changes on the CES. The changes will include enabling the RADIUS Service, making that service available, enabling the RADIUS Server, and updating profiles. Without making these RADIUS changes, your Contivity would be unable to communicate with the ACE Server for user authentication.

Contivity Step 1 – Enabling RADIUS Service.

1. Click SERVICES, RADIUS
2. Click "Add" under Clients.
3. Enter the IP Address of your ACE Server and a Shared Secret.

4. Then Click OK
5. Check "Enable RADIUS Service"
6. Under "Clients", check Enabled next to the Ace Server that you just added
7. Click OK.

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



Contivity Step 2 – Making RADIUS Service Available.

1. Click SERVICES, AVAILABLE
2. Under "Allowed Services", check Public and Private for Tunnel Type IPSec

3. Under "Allowed Services", check Public and Private for Authentication Protocol RADIUS

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

4. Click OK

Contivity Step 3 – Enabling RADIUS Server

1. Click SERVERS, RADIUS AUTH
2. Check "Enable Access to RADIUS Authentication"
3. Under "Server Supported Authentication Options", check Enabled for Type RESPONSE
4. Under "RADIUS Servers", for Server Primary
   A. Check Enabled
   B. Host Name or IP Address = ACE Server's IP Address
   C. Click the Radio Button for the Private Interface
   D. Port = 1645
   E. Secret = Secret used in Contivity Step 1.3
   F. Confirm Secret = Confirm Secret used in Contivity Step 1.3
5. Click OK
6. After completing changes to both CES and ACE Server, you can Click "RADIUS Diagnostic Report" under Diagnostics to check for errors in the configuration.

Contivity Step 4 - Updating Profiles

1. Click PROFILES, GROUPS

NOTE: Figure 2 below shows some Groups that I have setup. By default, there is only one Group, /Base. Group /Base should be your starting point when configuring profiles. Any settings that you want to use for all groups should be configured in /Base. Then you can add additional Groups under /Base. Under each Group, you can edit settings for Connectivity, IPSec, PPTP, L2TP, and L2F. This document will focus on the Connectivity and IPSec settings. Each Child Group created under Parent Group /Base can inherit settings from the Parent Group or can have custom settings defined. That way, you can use Child Group settings for authorization. This configuration allows ACE Server to determine a users Group based on the RADIUS Attributes received from the ACE Server after authentication.

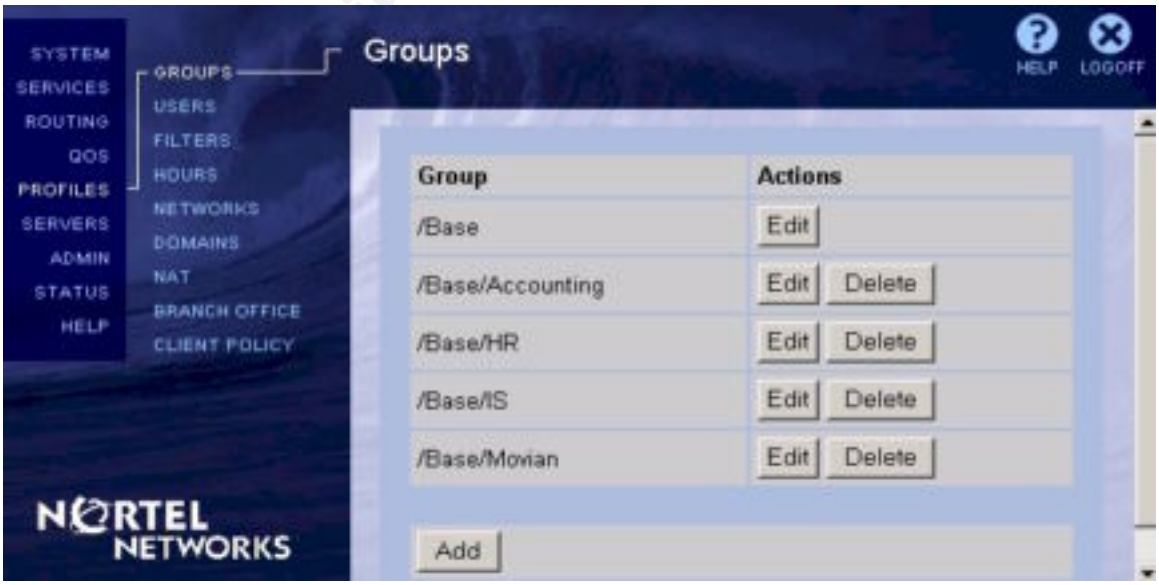


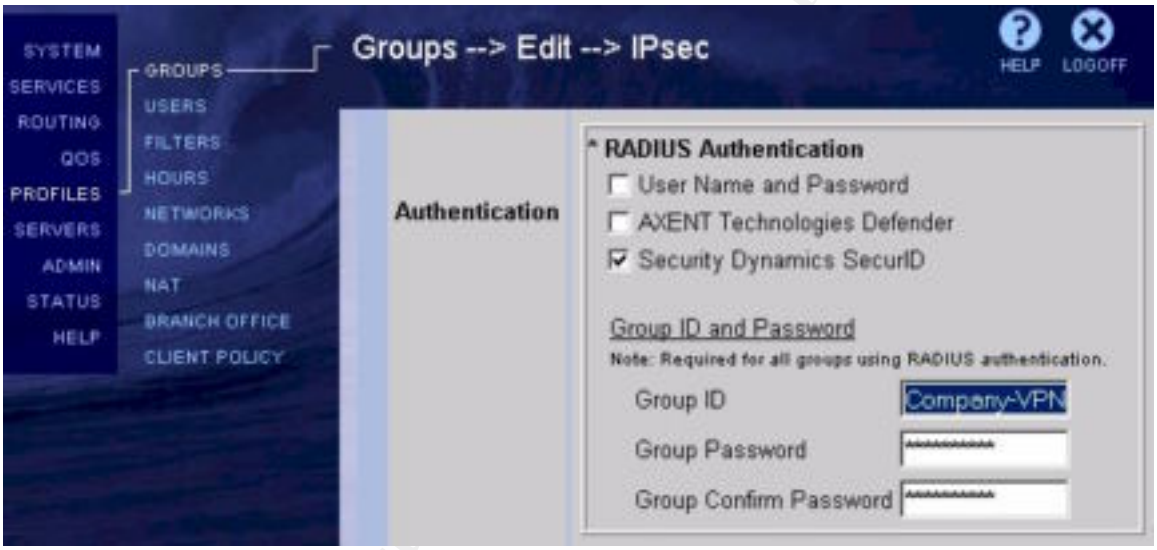
Figure 2. Sample Child Groups under Parent Group /Base

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

2. Click Edit for Group /Base
3. Under “IPSEC”, click Configure
4. Under “Authentication”, RADIUS Authentication**
    a. Check “Security Dynamics SecurID”
    b. Enter the “Group ID”
    c. Enter the “Group Password”
    d. Enter the “Group Confirm Password”

** Note: Setting the Group ID and Group Password under IPSec settings for /Base only, will allow you to make a single installation package. That way, you can use Nortel’s Custom Client Configuration setting and InstallShield’s EXE Builder to create the password protected, automated install.

5. Click OK



Optional IPSec Settings
Modifying the settings below for IPSec under /Base will make your Group configurations go much quicker. The IPSec settings tend to be static for all your groups. Where the setting for Connectivity under /Base/*ChildGroup* will be used for authorization.

- **Split Tunneling = Disabled**
  You cannot guarantee the security of your users home workstations. Therefore, you don’t want to allow them to be exposed to both the Internet and your network at the same time. Disabling Split Tunneling will prevent your network from being exposed to a potential backdoor.
- **Client Selection = Only Contivity Client**
  A single client will make your support staff’s life a lot easier. Allowing multiple clients would also defeat the purpose of creating a single, custom installation. You cannot take advantage of the authorization features that exist between your

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

ACE Server, Contivity Server and Contivity Client if you are not using the Contivity Extranet Client.

- **Banner = A warning about unauthorized used based on Security Policy**
  If your Security Policy already calls for a Login Banner for your LAN, you need to include one on your extranet connections. This will also help you with the legal issues in case of unauthorized access. Your users must click OK on the banner before being allowed to continue.
- **Display Banner = Enabled**
  What good is a having a Banner if you do not enable it?
- **Allow Password Storage on Client = Disabled**
  Since we are focusing on using SecurID Tokens for the Authentication method, passwords are single use only. No need to present your users with an option that will not completely work. If you allow the user to store the PIN on the client, you have just defeated the purpose of using Two Factor authentication.
- **Domain Name = domain.com**
  Enables you to specify the name of the domain that is used while an IPSec tunnel is connected. Specifying the domain name in this field ensures that domain lookup operations point to the correct domain. This is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server is mapped to the correct domain.
- **Primary DNS = your Primary DNS Server**
  This will allow your users to be able to resolve resources on your Network.
- **Secondary DNS = your Secondary DNS Server if applicable**
  This will allow your users to be able to resolve resources on your Network if the Primary is unavailable.
- **Primary WINS = your Primary WINS Server if applicable**
  Use this option for NetBIOS name resolution. It enables normal Windows File and Print Sharing to be accessed through the tunnel.
- **Secondary WINS = your Secondary WINS Server if applicable**
  This will allow WINS resolution if the Primary is unavailable.
- **IPSec Transport Mode Connections = Enabled (Required)**
  Use this option to either Enable or Disable IPSec.

Optional Connectivity Settings

To make authorization changes, modify the Connectivity settings for the Child Group. The Parent group values appear by default. Click the drop-down list boxes to change values. Modifying these settings based for the Group allows you to create different security policies based on the users role and needs. Appropriate use of Filters will allow you to take advantage of Nortel provided filters. It can also make use of custom Filters, the optional Stateful Firewall Filters, or Check Point Firewall-1 Filters.

- **Access Hours = Acceptable use hours for this Group**
  Specify the time ranges during which access is allowed for users in this group. The default value is Anytime.

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

- **Number of Logins = 1**
  Defines the maximum number of simultaneous logins IPSec clients in the group. Limiting this to 1 will deter users from sharing their account as well as being logged on in multiple places at once.
- **Password Management = Disabled**
  The ACE Server will handle all password management.
- **Idle Timeout = dd:hh:mm:ss**
  Enter an appropriate Idle Timeout in days, hours, minutes, and seconds format: dd:hh:mm:ss. The *Idle Timeout* is an amount of time a connection can be idle (no data has been transmitted or received through the connection for the specified amount of time). When the Idle Timeout expires, the session is terminated. This option helps prevent allocation of resources on the Switch for sessions that are no longer active. The default Idle Timeout is 00:15:00 minutes; the range is 00:00:00 to 23:59:59. The maximum number of days is 29. A setting of 00:00:00 specifies no Idle Timeout.
- **Filters = appropriate filter**
  The filters that appear in the drop-down list box are created using the Create Filter screen or have been supplied by Nortel Networks. Packet filtering controls the type of access allowed for users in a group, based on various parameters, including Protocol ID, Direction, IP addresses, Source, Port, and TCP Connection Establishment.
- **IPX = Enabled**
  Use this to either Enable or Disable support for IPX for each group.
- **Address Pool Name = poolname**
  The drop-down menu shows a list of Address Pools that have been defined. You can setup multiple pools to allow different Groups to get different sets of addresses. That way, if you /Base/IS users connect, they can get an IP Address that has appropriate rules defined on your network to allow access to restricted systems.

ACE Server Configuration Changes.

It is best to make these changes to the ACE Servers configuration from the console of the server. You will need administrative rights to the NT Server and administrative rights to the ACE Server Database.

ACE Step 1
You will need to edit the *hosts* file located in the /winnt/system32/drivers/etc directory. Using notepad, add entries into the *hosts* files for the 2 physical interfaces of the CES and the Management Interface too. Using the *hosts* file takes DNS issues out of the picture and ensures name resolution. Below is an example of entries in the *hosts* file:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# For example:
```

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

```
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
192.168.1.2   contivity2.domain.com      # CES Private Interface
192.168.1.3   contivity.domain.com       # CES Management Interface
63.100.47.46  vpn1.domain.com            # CES Public Interface
```

ACE Step 2

Adding the CES as a Client (Ace 4.1) or Agent Host (5.0x). The steps below are designed for Ace 4.1.

1. Click Start, Programs, ACE Server, Database Administration – Host Mode
2. In ACE DB Admin, Click Client, Add Client
3. Enter the following and click OK.
    a. Name: contivity.domain.com
    b. Network Address: 192.168.1.2 (CES Management Interface)
    c. Client Type: Communication Server
    d. Encryption Type: DES
    e. Open to All Locally Known Users: Check to allow any user to authenticate. Unchecked if you are going to use Groups Activations
4. In ACE DB Admin, Click Client, Edit Client, select "contivity.domain.com"
    a. Click Assign/Change Encryption Key…
    b. Enter Shared Secret Key used in Contivity Step 1.1 and Step 3.4
    c. Click OK
5. Without exiting the Edit Client Screen, Click Secondary Nodes…
    a. Enter contivity1.domain.com and Click OK
    b. Complete the Add Secondary Node dialog (CES Private Interface)
        i. Node name: contivity2.domain.com
        ii. Network Address: 192.168.1.3
        iii. Click OK
    c. Repeat Ace Step 2.5 but add vpn1.domain.com (CES Public Interface)
6. Click OK to exit the Edit Client Screen.

Ace Step 3

Setup Profiles to push the RADIUS Attributes to CES for Group assignment when authenticating.

1. In the ACE DB Admin, Click Profile, Add Profile
2. Enter the Name and following Attributes:
    a. Name: IS (Use Descriptive Name to denote CES Group)
    b. Class = ou=IS (this will match the /Base/IS Group)
    c. Framed-Compression = Van-Jacobsen-TCP-IP
    d. Framed-IP-Address = Select-by-NAS
    e. Framed-IP-Netmask = 255.255.0.0 (based on your Network Scheme)
    f. Framed-MTU = 1500
    g. Framed-Protocol = PPP
    h. Framed-Routing = None

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

i. Service-Type = Framed
3. Click OK
4. Repeat Ace Step 3 as needed for each CES Group you created.
5. Assign the Profile to the appropriate user as needed.

Contivity Client Configurations
The following changes must be made on the Contivity Client to allow Authentication using RSA SecurID tokens.

CES Client Step 1
1. Launch the Nortel Networks Contivity VPN Client
2. Click File, Connection Wizard
3. Enter the name for this connection profile: Company VPN, Click Next
4. Select Hardware of Software Token Card, Click Next
5. Select Response Only Token Card, Click Next
6. Enter the following and Click Next:
    a. User ID for the Token Card
    b. Token Group ID (same Group ID from Contivity Step 4.4b)
    c. Token Group Password (same Group Password from Contivity Step 4.4b)
7. Enter the Host Name or IP Address for the VPN server, Click Next. (This would be either the CES Public or Private Interface address. Or you can setup DNS to use a host name.)
8. Select, based on your preference, either "No, I do not want to dial first." or "Yes, I want to make a Dial-up connection first.", Click Next
9. Click Finish to complete the Connection Wizard.
10. Click Options, Authentication Options
    a. Group Authentication Options, Response Only Token, Options>>
    b. Check Use Passcode Display
    c. Click OK

Customizing the Contivity Client Files for Automated install. (Optional)
If you have already configured one client and have added all the connection information to it, such as name of connection, IP address of the switch, Authentication Options, etc. and are satisfied that it is ready for general distribution, go to the traditional Program Files\Nortel Networks directory and copy the ***Baynet.tbk*** *file into your custom directory. This file can be edited with Notepad. Example of the entries would be as follows:*

[Company VPN]
Description=
Dialup=(None)
Username= you would leave this blank for the user to add after the install
UseTokens=1

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

TokenType=2
UsePAPGroup=1
GroupName=Group name would go here
SavePassword=0
Server=DNS Name or IP Address of Public Interface side of switch

Note that the TokenType can be any of the following:
0=Username/password authentication
1=Axent hardware token
2=Security Dynamics hardware token
3=Radius authentication
4=Axent software token
5=Entrust certificate

There is a setup.ini file in your custom directory that by default only has the following:

[Startup]
AppName=Extranet Access Client (You can change this to suit the client needs)
FreeDiskSpace=511

You can add Options:

ProductName=	Whatever name you want to show up on the Programs Menu
FolderName=	Where under Program Files do you want the application to reside
NoCMIcon=1	If you don't want the option of the Connection Manager listed under the Start-.Programs Menu, 0 if you do.
NoPWIcon=1	If you don't want the option to change CES access passwords available. 0 if you do.
NoChangeProfiles=1	Prevents users from modifying anything within the client, except user id, password and dialup options.
SkipScreens=1	Bypasses the Readme file.

[Options]
ProductName=VPN Client
FolderName=VPN
NoCMIcon=1
NoPWIcon=1

AddDesktopShortcut=1	If set to 1, a shortcut Icon will be added to the desktop
GroupIniFile=group.ini	
ClearDNS=1	This feature speeds up the tunnel connection process by querying the correct DNS server for the tunnel, rather than first attempting to query a public DNS server that is used for non-tunnel traffic.

There is a group.ini file in your custom directory that by default only has the following:
[ProfileNames]

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

1=Company VPN	This name MUST match exactly the profile name found within the baynet.tbk file
[Nortel Demo Install]	
GroupPW=mygrouppassword	Whatever that password should be under authentication Option
NoSavePassword=1	Prevent the user from trying to save his personal password or Pin.

Copy the setup.ini & group.ini files into your custom install source directory.

Download from the web, InstallShield. It's free and it's one self extracting exe file which will automatically ftp setupex.exe to wherever you want to save it to on your hard drive.[8]

http://support.installshield.com/resource/exe_builder.asp

Run the setupex.exe and it will setup InstallShield on your PC. Once installed, run InstallShield EXE Builder to complete your custom Installation Client. The exact user of the InstallShield EXE Builder is outside the scope of this document. However, the application is self-explanatory.

Conclusion

A VPN is one of several cost-effective mechanisms for supporting the extranet's communication backbone by utilizing the Internet. With more and more company deploying VPNs, you want a solution that is going to be secure and flexible. They can be created using software, hardware, or a combination of the two that creates a secure link between two peers over a public network. This is done through encryption, authentication, packet tunneling, and firewalls.[9] Nortel's Contivity coupled with RSA's ACE Server provides you with a design that is going to be tough to beat. Their features compliment each other to ensure a successful VPN solution. Their authentication and authorization capabilities provide for a secure extranet and gives your users something that is easy to use. More then 10 million people use RSA SecurID authenticators to securely access virtual private networks, remote access firewalls, Web applications and network operating systems. The system is easy to use and manage and results in centrally enforced security with an immediate ROI in any e-business initiative.[10] Nortel Networks is a leading vendor in IP VPNs. Utilizing their success, managers can almost be ensured of a seamless deployment with a maximum ROI. Providing that solution not only gives you some job security, it improves your chances of your future projects being approved. So, once you get your VPN secured, move on to the rest of your network to make better use of all the money you just spent.

[8] INST
[9] OREIL
[10] RSA2

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

References

Online:

[THUR] Thurman, Mathias **"**Management finally backs a security analysis of a new VPN; now Mathias Thurman just needs a plan." Security Management Journal. 10 September 2001
URL: http://www.sans.org/newlook/resources/SMJ/091001.htm

[NORT1] Nortel Networks Inc. "Contivity Secure IP Services Gateway Portfolio." Best in class IP VPN. Copyright 1999
URL: http://www.nortelnetworks.com/products/01/contivity/benefits.html

[FVPN] www.findvpn.com "About Nortel Networks VPN Services" Copyright 2000, 2001, 2002.
URL: http://www.findvpn.com/providers/nortel.cfm

[NORT2] Nortel Networks Inc. "Contivity Secure IP Services Gateway Portfolio Brief." Technical specifications – corporate/enterprise models. 02 April 2002.
URL: http://www.nortelnetworks.com/products/library/collateral/55129.02-04-02.pdf

[HULME] Hulme, George V."RSA Boosts Two-Factor Authentication Management." RSA Security upgrades its ACE/Server software. 1 June 2001.
URL: http://www.informationweek.com/story/IWK20010601S0002

[RSA1] RSA Security Inc. "RSA SecurID". Compatibility with your Infrastructure. 2002
http://www.rsasecurity.com/products/securid/tokens.html

[INST] InstallShield Corp. "EXE Builder" 14 August 1996.
URL: http://support.installshield.com/resource/exe_builder.asp

[RSA2] RSA Security Inc. "RSA SecurID Authenticators". The gold standard in two-factor user authentication. May 2002.
URL: http://www.rsasecurity.com/products/securid/datasheets/SID_DS_0502.pdf

Books:

[NICH] Nichols, Ryan, & Ryan. Defending Your Digital Assets, Special Condensed Edition. McGraw-Hill and RSA Press. Pages 142-143

[OREIL] Scott, Wolfe, & Erwin. Virtual Private Networks, 2nd Edition. O'Reilly and Associates Inc. January 1999. Page 2

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

Last Updated: September 26th, 2017

Upcoming Training

SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
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 St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
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
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
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
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor