Global Information Assurance Certification Paper

GIAC Certification
GSEC Practical Version 1.4b
Option 2

Matthew Hall
Submission Date:

Robust IPSEC Based Corporate Infrastructure Deployment Using The Nortel Contivity Switch
A Deployed Case Study

Abstract

The use of IPSEC VPNs (virtual private networks) to replace classic frame-relay and leased line corporate infrastructure is becoming an increasingly common occurrence in the enterprise environment. There remains, however, a large list of concerns with implementation and reliability that many enterprise products on the market are attempting to address. Nortel's line of VPN concentrators, known as Nortel Contivity Extranet Switches, have a long list of features that can be utilized to provide an enterprise level of service to organizations wishing to take advantage of the cost savings provided by a VPN based infrastructure, without having to make significant sacrifices to the current security and availability of their legacy solutions.

Contained in this case study is a chronicle of the actual deployment of an IPSEC VPN based infrastructure using Nortel Contivity VPN concentrators. It follows hardware implementation decisions and research, planning of the infrastructure, technology decisions, testing stages, implementation and refinement, and future technologies that will allow for further improvement. In addition to technical considerations, policies play a strong role in a successful and stable implementation; and thus will be covered during all phases of the deployment. Due to budget and usability constraints, no single all reaching solution for any one give problem could be reached. For this reason, defense in depth was key to solving the complex problems involved in the deployment. Access control, intrusion detection, redundancy, security policy, and physical security all had to come together to provide the best availability possible.

Planning and Requirements

Loss of availability was going to be the primary and overriding risk that I would attempt to focus on during the planning and implementation stages. Any threat to this had to be minimized. There are several vulnerabilities and threats that can put availability at risk, and the solution would attempt to mitigate these risks where ever possible.

Vulnerabilities:
Single points of failure due to hardware or ISP connectivity
Minimal bandwidth on WAN links that is subject to saturation
Physical security at remote locations
Logical security of services running on the Contivity Switches
Multiple ingress and egress points to the private network
Dynamic routing protocol vulnerabilities

Threats:
Denial of Service attacks aimed at the VPN Concentrators
Virus infestation and proliferation
Trojan horses

Insecure publicly available hosts
Brute force attacks or management traffic monitoring aimed at compromising management passwords
Unauthorized user tunnels
Unauthorized password recovery attempts
Spoofed routing protocol updates
Human error

Hardware Redundancy

Redundant hardware is the obvious solution for single points of failure, but this brings up as many questions as answers. How would traffic be redirected to the second device in case of a failure? In the primary locations, it was decided that OSPF (a dynamic routing protocol) would be used to route traffic between the devices. Nortel Contivity Switches not only allow for OSPF on the internal interfaces, but can negotiate VPN tunnels using OSPF or RIP encapsulated in IKE. This allows for smooth integration into a preexisting OSPF or RIP infrastructure and allows for the addition of new subnets to locations without any reconfiguring of the VPN tunnels.

At branch locations, host machines would point at the Contivities directly for their default route; this meant that OSPF would only be a viable solution for tunnel negotiation. Instead, VRRP would be used to share the IP address of the default route of these hosts. VRRP is a standards based protocol that can be used to allow multiple devices to share an IP address and take ownership of it if either connectivity is lost to a device, or a monitored interface on a device goes down. Nortel provides for a feature called “Interface Groups”, that can be used to monitor multiple VPN tunnels, and cause a failover of the VRRP address, only in a situation where all of the VPN tunnels on a device have failed. This minimizes the risk of false positive failover if WAN connectivity is still available but a single remote tunnel goes down.

Backups were taken of the configuration and stored on a secure network services server with restricted access. In addition, the Contivity switches can be configured to perform regular self backups. These use ftp to push scheduled backups to designated servers. Backups can be set for only certain days and times of the week or at preset intervals. In addition, partial backups may be chosen as an alternative to full system backups. In this case, intervals would be set to once every five hours and only configuration file backups would be taken.

ISP Redundancy

Redundancy at the ISP level was the next step in planning. Without redundant links to the internet, a single problem with an ISP could cause the entire infrastructure to fail. Although ISPs provide SLA’s (Service Level Agreements) on the more costly links that provide service to the main locations in the

infrastructure, it is still advisable to have a secondary link to the internet. At the main offices, a second service provider was used to provide connectivity, and BGP was used to advertise the IP address range over both ISPs. This would ensure that no single ISP infrastructure could cause a loss of connectivity; in addition, BGP allowed us to maintain a single set of IP addresses, and thus allowed both primary and failover hardware devices to take advantage of the ISP redundancy.

In the remote offices, however, connectivity was far more difficult to provide. In most cases, DSL was not an available option. DS1 lines were purchased instead. The only options for link redundancy were IDSL or ISDN in many cases, and the bandwidth requirements of these locations ruled out these options. Due to the high SLA on DS1 links and the less mission critical nature of the locations, it was decided that the budget could not be justified for a second or even partial DS1. This caused a collapse of the above stated wishes for hardware redundancy in these locations. Budget for a second device was taken up by the more expensive DS1 connection, so a compromise was reached. Fortunately, the Nortel Contivity switches can directly terminate WAN connections of many different types so a border router in these locations was not needed. Instead, the budget saved from this device would be put towards 4 hour maintenance contracts on the Contivities at these offices (a luxury that was only planned for primary locations). In the case of hardware failure, a new device would be on hand in 4 hours or less. This allowed for some mitigation of the risk associated with single points of hardware failure at these locations. In other locations, DSL links were used as a means of failover. These low cost links provide large amounts of bandwidth without the associated SLA's of more expensive, traditional services. They were deemed sufficient for backup use.

In very small, non critical offices, DSL or Cable modem services were used for connectivity. In these cases, the impact due to any loss of availability was not high enough to justify the cost of more expensive DS1 services or redundant hardware

Obviously, cost is a barrier to both hardware and ISP redundancy, so sizing both the Contivity switches and the bandwidth of the links appropriately was of great importance. Over sizing the devices and links slightly for growth was acceptable, but beyond that no added benefit from larger links and hardware would be seen. In fact, the only associated difference is an increase in cost. Throughput and performance numbers on the Contivities are proprietary data, but Nortel was more than helpful in providing the information needed to size these devices. Contivity 1100s were chosen to terminate most DSL and DS1 links, and 1700 class devices were chosen to terminate the DS3 links at primary locations.

Bandwidth Saturation

Remote offices are normally connected using low bandwidth links that can easily be saturated by even one compromised system on a 100 or even 10 megabit LAN. Some safeguards had to be in place to prevent any malicious or even innocent traffic from saturating these links. The Nortel devices provide for different options in the way of QOS (quality of service) on both the tunnels and physical links. These include RSVP, DSCP and internal Bandwidth management. In addition, a stateful firewall on each device is provided. The flexibility of this firewall is key to securing and controlling traffic. It treats each tunnel as a separate interface that can be filtered for both egress and ingress traffic in addition to the physical interfaces themselves. Filters would be put into place for nonessential traffic to help lower bandwidth usage and mitigate risks associated with non used and dangerous protocols such as the rcommand set of tools. We could also filter traffic in an emergency situation to prevent the proliferation of virulent traffic and to "quarantine" locations. It was at this point that the use of policy played its first major role. A policy was drawn up to provide for emergency response and termination of service to hosts whose traffic was threatening the network infrastructure. Some of the key points are listed below.

1. Upon discovery of malicious or innocent traffic that threatens to bring connectivity below acceptable service levels, that traffic is immediately subject to termination or filtering.

2. Network staff will first make an attempt to contact the Director of Network Services to gain approval to terminate traffic.

3. If the Director of Network Services is unavailable, the network staff member may proceed to filter or terminate traffic after consulting with at least one senior member of the network services team.

4. After termination of traffic has been successfully accomplished and service levels returned to normal, the network staff member will then make attempts to contact the owner of the system in order to inform them of the subsequent termination of traffic.

5. Network services to the host will be restored in a timely manner as soon as the offending traffic is terminated by placing a request for reinstatement using the company's call management system.

This begs the question, how do you find this traffic? A commercial network IDS (Intrusion Detection System) is to be placed at the central office to monitor all ingress and egress traffic on the internal network. In addition, core routers at the central office are to be configured using NetFlow caching to provide additional tools for network staff to find the source of malicious traffic. NetFlow caching is an excellent feature provided by Cisco routers and adds little to no overhead to performance.

"NetFlow provides valuable information about who is using the network, what applications are used, when the network is utilized and where traffic is going on the network."[1]

Configuration of NetFlow caching is beyond the scope of this document.

The Contivity supports compression on all tunnels and it will be enabled in all cases in order to gain any possible bandwidth savings that it can provide.

Finally, Server Admin teams deployed a standardized Anti Virus Solution to all hosts. It provided for centralized virus definition updates, as well as the centralized reporting of virus infestation. The reporting could be used to proactively limit and quarantine virus proliferation to certain segments of the network early on in the infestation, and thus prevent problems from escalating to a corporate wide impact.

This is far from a perfect solution; but following the defense in depth model, many possible deterrent and detection methods were used to try and mitigate the risk involved with this vulnerability, which proved to be the most commonly experienced problem in the infrastructure.

Physical Security

An obvious danger presents itself when critical service devices are placed in a remote location with little or no supervision. In the larger locations, we were able to mitigate the risks by providing a locked facility that could store our devices. Badge readers were primarily used, although simple physical keys were used at the smaller locations due to budget. Only select personal were provided access to these devices, and again policy played a role in the securing of these facilities. Below are a few key points.

1. Only the personnel authorized with access are allowed into the secure IT lab or IDF.

2. Personnel with access to the secure IT lab or IDF are only authorized to enter these restricted areas with prior IT permission or at the request of IT personnel.

3. A request must be made to IT personnel for each instance of access needed to restricted areas.

[1] Cisco Systems, Inc. "Cisco IOS Software NetFlow." 1992 – 2004. URL:http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml (11 June 2004)

4. Restricted IT areas must be clearly marked and a method access control must be placed on the entryway of the area that coincides with previously acceptable policies.

Although obscurity is not security, it does assist in providing some risk mitigation to these areas, thus it was attempted to prevent the need for anyone to enter. In line with the goal of availability, out of band management was provided to most of the locations using devices from Baytech. These devices provide remote power management, for hard reboots of the network devices, as well as remote console access. They are accessible via IP or dialup modem, and both methods were secured with strong passwords and user login IDs. Multiple user IDs and permissions can be created on these devices; but stand alone, their security is not insurmountable. Fortunately, the power management section of the device utilizes a second set of authentication credentials. All of the Nortel Contivity devices require a login and password for entry into the out of band management port. This additional line of defense provided for some depth to security at these locations.

The Nortel Contivities themselves are very resilient to physical security breaches. Only the Primary Administrator account can log into the Contivity via the out of band port. Even user accounts with administrative rights lack this ability. In addition, there is no password recovery process for the administrative account. If the account password is lost or forgotten, the Contivity has to be RMAed for a replacement from Nortel. So there are no risks of unauthorized password recovery attempts, similar to those that can be exploited on Cisco routers. SNMP traps were to be setup on the Contivities to track failed login attempts. Traps could then be filtered for the administrator account login failures, so that any brute force attempt at password recovery could be detected (a strategy that was also used with the logical security of the device).

Vulnerability of the physical cabling to tapping and sniffing is something that is unavoidable except through physical access restriction as stated above. However, the most secure means possible were used to avoid making management traffic easily accessible.

Logical Security

The Nortel Contivity Switches come with a standard configuration that is admirably secure. Basic security starts by setting an interface as either public or private. Public interfaces will not advertise any services other than the VPN protocols that are supported on the device. All protocols accept for IPSEC would be disabled. Private interfaces accept management traffic and dynamic routing protocols (if configured) as well. This can be further refined by disabling any unused management services.

If the Contivity Stateful Firewall license is installed, it provides for an easy to use system of traffic filtering. Without it, simple access lists (filters) must be used on a per interface basis. It can be configured through the command line, or through a java applet graphical interface, very similar to the classic Check Point firewall interface. In addition, the Contivity switches can actual run Check Point firewall itself (which would not be used in our case). The Contivity Stateful firewall treats all tunnels as separate physical interfaces, and allows for filtering decisions to be made at all points in the routing process through the switch. It provides a powerful NAT (Network Address Translation) system that allows for the NATing of tunneled and non tunneled traffic. All firewall rules can be set to log, in varying detail, each match of a particular firewall rule to the internal Syslog and any configured external Syslog server. All rules also carry the option to send SNMP traps to any Configured SNMP receiver in the event of a rule match.

ICMP echo requests would be the only additional service allowed to contact the public interfaces of the Contivities (for monitoring and testing purposes). Matches to this firewall rule were logged in order to monitor for any flooding.

Internally, only IPSEC, Telnet, FTP, HTTP and SNMP services would be enabled on the private interface. The use of such insecure protocols on a security device was disheartening. Especially considering there were no secure options, but traffic was none the less secured with a little creativity. The Contivity itself has a separate IP address for management activities that is completely separate from the IP used for routed traffic across the device. This allows for filtering of management traffic, using the stateful firewall. Using this, we were able to protect the normally insecure http, telnet, and ftp management traffic by allowing it only from a specific user VPN tunnel group. This VPN group, in which the administrative logins of the senior network services staff would reside, could be filtered using the Stateful firewall as a logical interface much like a branch office tunnel. Senior staff could then use the Nortel VPN client to create an IPSEC tunnel to the Contivity and access the management interfaces securely. In addition, since the tunnel group itself was allowed access, and not a specific set of IP addresses, there was no danger of access via spoofed IPs or local physical security breach.

SNMP monitoring was enabled using both Get queries from an enterprise management console, and traps that were sent out to the same system. The Contivity itself primarily uses SNMP version 1, which does not provide for as much security as would normally be desired due to it's use of simple plain text community strings. However, features in the Contivity allowed for some security to be had. The Contivity itself does not accept any SNMP Set commands, meaning that no remote configuration can be performed on the Contivity using SNMP, only monitoring. SNMP servers have to be specified by IP address in addition to a community string. This allows for IP based filtering of the SNMP Get requests themselves. There will always be the danger of spoofed IP

requests, but the benefits of SNMP monitoring were found to out weigh the potential risks involved.

The Contivities were to be configured to send traffic to external Syslog servers in addition to logging traffic to their own internal hard drives. This provided for redundancy in the logged data, as well as a means to check for any log tampering.

User accounts were to be created for each senior member of the networking staff and were given management rights to the switch. In order to increase accountability and track human error, the Primary Administrator account was to be used for management of the switches only in the event of an emergency that required direct out of band console access. Change management policy was to be put into place requiring all changes go through a team approval and refinement process prior to final Director approval. Changes would then be performed during preset maintenance windows with rollback procedures and set time limits. These policies would go into place in an effort to minimize human error.

Multiple Network Ingress/Egress Points

The problem with internet connectivity at each office location is the fact that each office location suddenly became another entry or exit point to the network. The more entry points into the network; the harder and more complex an infrastructure becomes to secure. The solution to this problem is was quite simple; eliminate these entry and exit points. The Nortel Contivity switches carry two separate default routes, an external and an internal. In this case, the external is the ISP provided default route; and the internal will be injected via OSPF. IPSEC traffic and other "external" based switch traffic always uses the external default route, but traffic that sources from private interfaces has the option of using either default route. By setting the internal default route as the preferred route, under the routing configuration section of the Contivity, all traffic destined for non local networks is encapsulated and routed across the tunnel to the central office. With all traffic being tunneled to the central office, these locations ceased to be Ingress/Egress points into the network. In addition, all traffic can be secured using any preexisting, centralized infrastructure. Although this does mean a larger load on central office internet links, it was deemed to be worth the added benefits to security and uniform policy enforcement that it provided.

Dynamic Routing Protocol Vulnerabilities

> "The friendly nature of OSPF dictates that any router with coordinated configuration parameters (network mask, hello interval, dead interval, etc.) can participate in a given OSPF network. Because of this default behavior, any number of accidental factors

(misconfigurations, lab machines, test setups, etc.) have the potential to adversely affect routing in an OSPF environment."[2]

With the use of dynamic routing protocols, there always comes the risk of exploit. These can be either malicious or innocent in source, but their affect can be far reaching and corporate wide. In an attempt to prevent unauthorized route updates, that could disrupt the infrastructure, md5 authentication will be used to authenticate OSPF updates. This is by no means a perfect solution but will provide a greater level of security than a default deployment. Unfortunately, the Contivity provides no option for nonbroadcast mode OSPF which would provide for increased security.

We do however have one other option to increase security of the OSPF deployment. This lies in the stateful firewall. OSPF uses multicast to communicate in broadcast mode so we have no way of filtering outgoing advertisements, but we can, however, filter incoming based on their source IP address. In addition, we can filter any outbound OSPF advertisements altogether on LAN segments that have no participating routers.

Implementation

Basic configuration of the Contivity switches, including switch setup and basic tunnel configuration are covered in great detail in the documentation guides at Nortel's website and is below the scope of this case study. Please refer to the documentation links provided in the references section for basic information.

Instead, the focus will be on the specific configurations required to secure the system. We chose to use version 4.75_140 of the Contivity Code, and all configurations were first tested in Nortel's onsite lab facilities in Richardson, TX prior to deployment in the enterprise.

Securing the Contivity

Services

The first option that is of note is the services -> available menu. This is where we will set the majority of the advertised services on the Contivity. In this case, the Contivity switches will be setup to accept only IPSEC tunnels on the public and private interfaces, and HTTP, SNMP, FTP, and TELNET management traffic on the private interface only.

Allowed Services

[2] Chan, Jason. "Secure Routing?!?" Securing OSPF. February 2001. URL: http://www.liquifried.com/docs/security/securingospf.htmlb (11 June 2004)

Tunnel Type	Public	Private
IPsec	☑	☑
PPTP	☐	☐
L2TP & L2F	☐	☐

Management Protocol	Public	Private
HTTP		☑
SNMP		☑
FTP		☑
TELNET		☑
Identification		☐
CRL Retrieval	☐	☐
CMP	☐	☐
RADIUS Accounting	☐	☐

Authentication Protocol	Public	Private
RADIUS	☐	☐

Next, in the Services->IPSEC menu, we will limit the types of ciphers allow on the system as well as the authentication types.

Authentication

User Name and Password/Pre-Shared Key	☑
RSA Digital Signature	☐

RADIUS Authentication

AXENT Technologies Defender	☐
RSA SecurID	☐

User Name and Password	☑

Encryption

ESP - AES 128 with SHA1 Integrity	☑
ESP - Triple DES with SHA1 Integrity	☑
ESP - Triple DES with MD5 Integrity	☐
ESP - 56-bit DES with SHA1 Integrity	☐
ESP – 56-bit DES with MD5 Integrity	☐
ESP - 40-bit DES with SHA1 Integrity	☐
ESP – 40-bit DES with MD5 Integrity	☐
ESP - NULL (Authentication Only) with SHA1 Integrity	☐
ESP - NULL (Authentication Only) with MD5 Integrity	☐
AH - Authentication Only (HMAC-SHA1)	☐
AH - Authentication Only (HMAC-MD5)	☐

IKE Encryption and Diffie-Hellman Group

56-bit DES with Group 1 (768-bit prime)	☐
Triple DES with Group 2 (1024-bit prime)	☑
Triple DES with Group 7 (ECC 163-bit field)	☐
AES 128 with Group 5 (1536-bit prime)	☑
AES 128 with Group 8 (ECC 283-bit field)	☑

Because we will not be using RSA Digital Signatures or Public key cryptography in our implementation, I have disabled it. The decision was made to use preshared secrets due to the limited scope of the deployment, and the complication and expense of setting up a Public Key Infrastructure. IKE negation and its use of Diffie Hellman exchanges ensured that the preshared secret will never even transmitted across the network.

"A Diffie-Hellman exchange works like this: two people

> independently and randomly generate values much like a public/private key pair. Each sends its public value to the other (using authentication to close out the man-in-the-middle). Each then combines the public key just received with the private key just generated, using the Diffie-Hellman combination algorithm. The resulting value is the same on both sides, and therefore can be used for fast symmetric encryption by both parties. But no one else in the world can come up with the same value from the two public keys passed through the net, since the final value also depends on the private values, which remain secret."[3]

As a result, the preshared secrets had to be maintained securely and encrypted on a network services secured server. Only senior network staff would have access to these preshared secrets and policy dictated that they were changed on an annual basis or when there were any changes to the senior network staff.

Only the required ciphers were enabled on the Contivity switch. EAS 128 with SHA1 Hashing would be used for all branch office tunnels. This decision was made due to that fact that all encryption would be done in software without using the use of Nortel's option hardware based encryption cards.

> "The AES is the Advanced Encryption Standard. The AES was issued as FIPS PUB 197 by NIST (see Question 6.2.1) standard is the successor to DES (see Question 3.2.1). In January 1997 the AES initiative was announced and in September 1997 the public was invited to propose suitable block ciphers as candidates for the AES. The AES algorithm was selected in October 2001 and the standard was published in November 2002. NIST's intent was to have a cipher that will remain secure well into the next century.
>
> AES supports key sizes of 128 bits, 192 bits, and 256 bits, in contrast to the 56-bit keys offered by DES.
>
> The AES algorithm resulted from a multi-year evaluation process led by NIST with submissions and review by an international community of cryptography experts. The Rijndael algorithm, invented by Joan Daemen and Vincent Rijmen, was selected as the standard."[4]

---

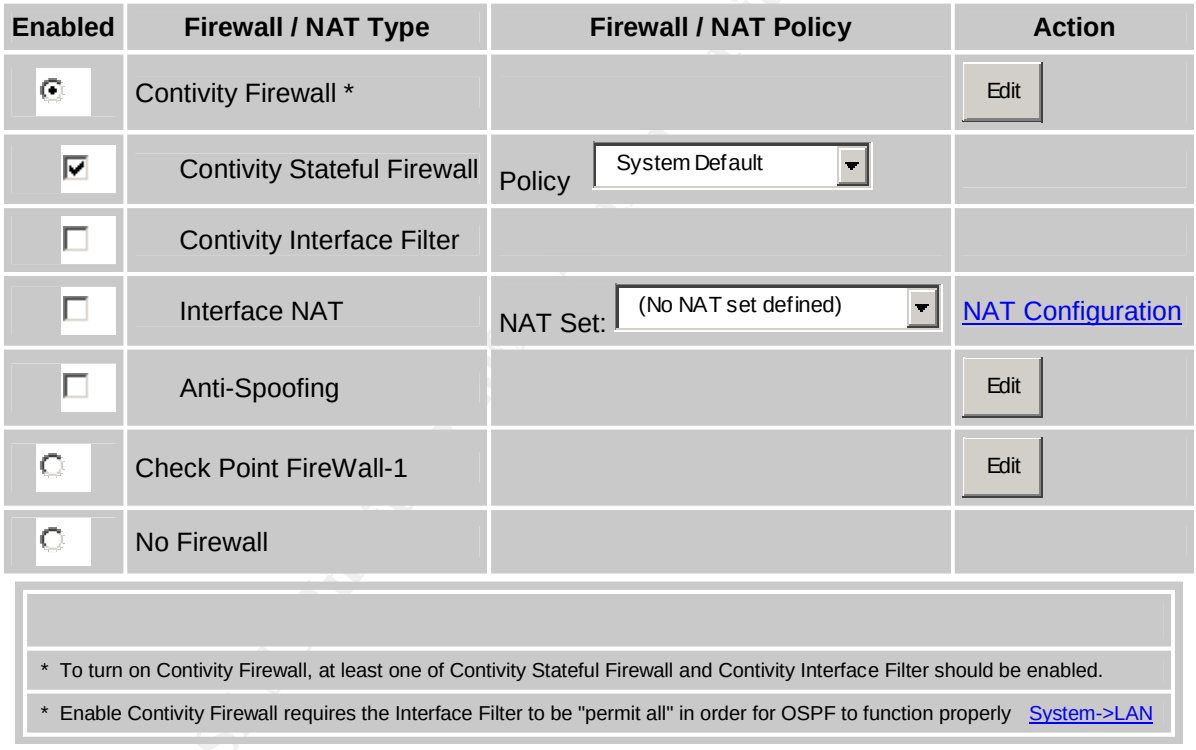
[3] Alcatel. "Key Management and Exchange." Understanding the IPSec Protocol Suite. 2001. URL:http://www.cid.alcatel.com/doctypes/technewbridgenote/pdf/ipsec_nn.pdf;$sessionid$BM1G5FQAABCKPQCLC3GHBM2KPBUSQ2G0 (11 June 2004)

[4] RSA Security. "What is the AES?" Techniques in Cryptography. 2003. URL:http://www.rsasecurity.com/rsalabs/node.asp?id=2235 (11 June 2004)

All Nortel switches come with powerful Intel based CPUs and relatively large amounts of ram. Because of Rijndael's ability to be easily handled by Intel's x86 class of CPU's, it provides better through put than 3DES which was our other alternative for secure data encryption levels that were to be considered. DES was deemed too insecure for current implementations. Triple DES encryption with SHA1 hashing was still enabled on the switch but only for use in the user tunnels. The reasons for this were quite simple, at the time of implementation the Nortel user client would not perform AES based encryption. The IKE and Diffie-Hellman Groups were chosen for similar reasons.

Firewall

Next, the services -> firewall/NAT menu was accessed.

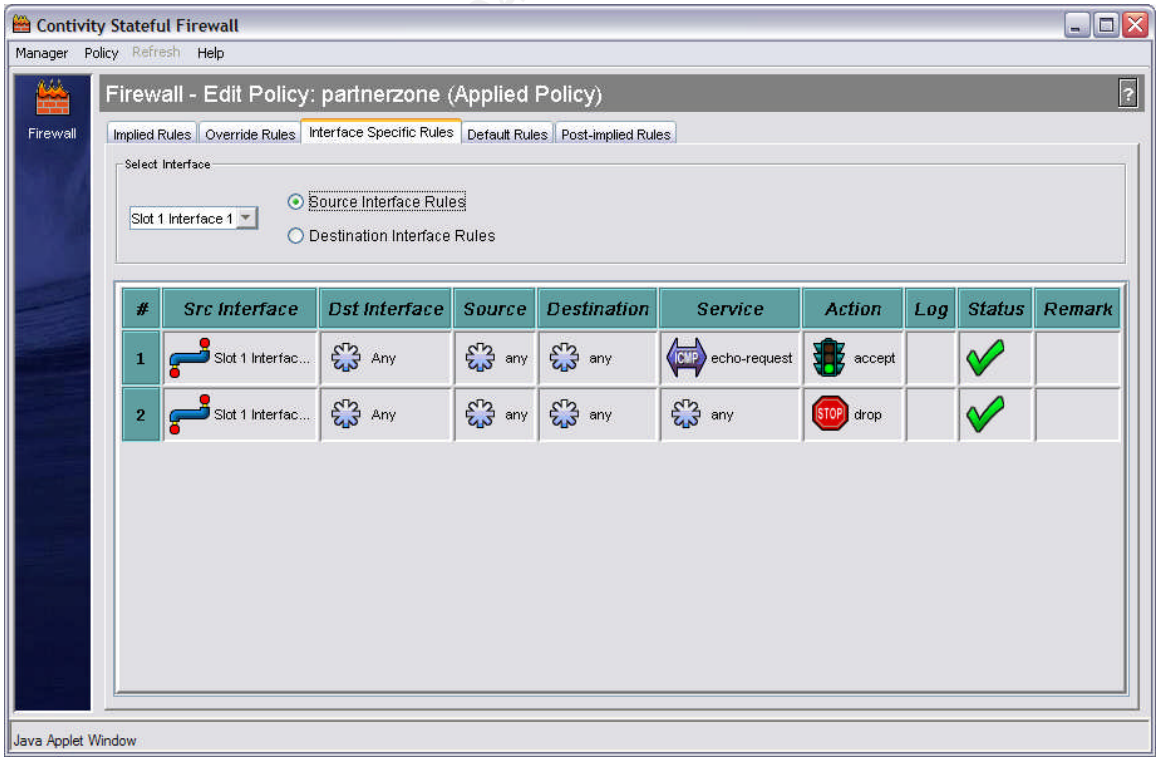


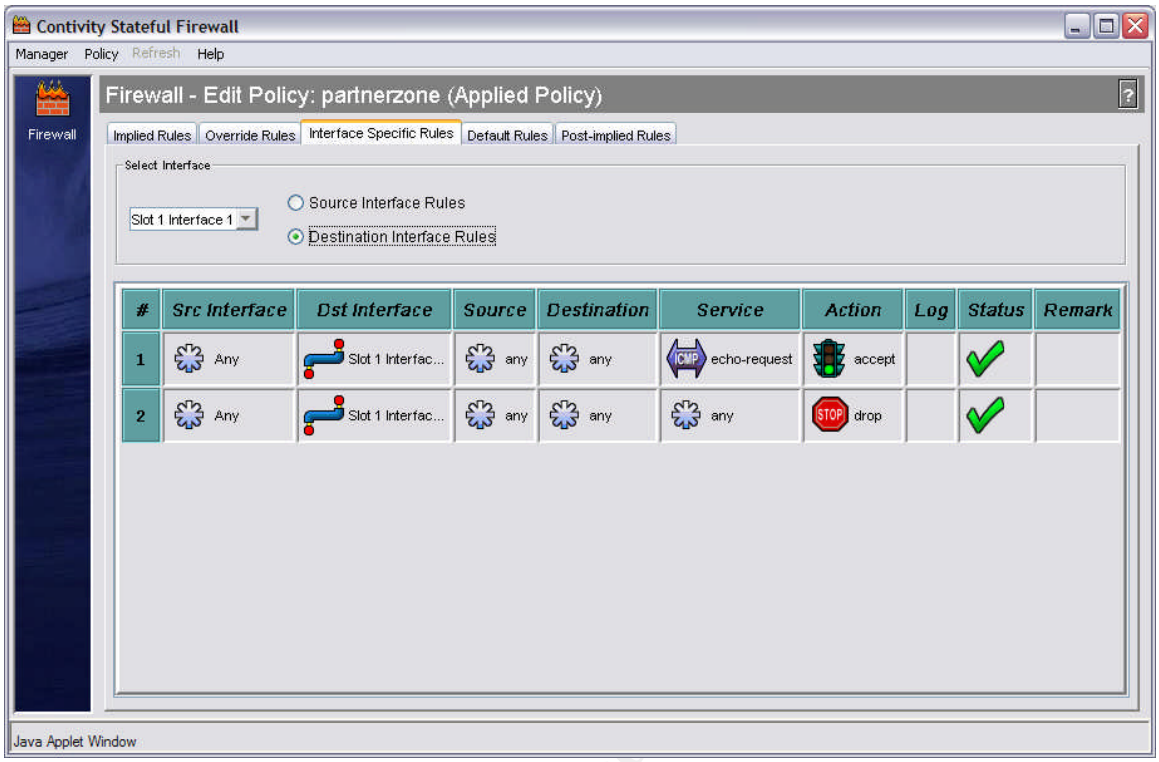
The Contivity Firewall was enabled, and Contivity Interface Filters and Contivity Tunnel Filters were disabled since they would not be needed with the firewall in use. The Anti-Spoofing feature provides protection against certain types of spoof

attacks and is enabled for an extra measure of security. A reboot of the switch is required to enable the firewall and thus was performed at this time.

Clicking the “Manage Policies” button next to the current policy brings up a Java based console for editing the firewall policies. The firewall policy for a system such as this can be quite large, so rather than display the entire policy a few example rules will be provided below to show the granularity provided by the firewall.

There are several tabs in the editor, and all rules are applied across the system in order from left to right as you move across the tabs. Implied rules are not editable, and are provided by the system for management and tunnel protocols to be allowed to the system by default. Override rules are user editable and are system wide. They are best used for trouble shooting. For example, by placing an allow all rule in in the override rules section, it may be possible to rule out firewall policy as a cause for loss of connectivity. Interface rules provide the ability to apply specific ingress and egress policies to each physical interface, in addition to each branch office and user tunnel group, which appear as virtual interfaces. Below is an example of a rule allowing echo requests both in bound and out bound from the Contivity’s public interface. Note the ability to filter not only on IP, but by source and destination interface/tunnel as well. Rule logging options are also entered here. There are options for none, brief, or detailed logging to Syslog, in addition to trap, which will send an SNMP trap to any configured trap servers.





Remember that this is a stateful firewall, so the state of outbound traffic will be held to allow replies back into the firewall automatically. Hence, there are no rules allowing echo replies back into the firewall. The Default Rules tab allows for any final defaults to be set by the administrator. The final tab, Post-Implied rules, is another non user editable tab providing for management services and the like.

Multiple policies can be stored on the Contivity, and they can be copied and changed for revision control. Note that only one policy can be applied at one time.

Under the Admin –> Administrator menu it is possible to change the Primary Administrator account ID and set a new password, which is highly advisable.

Primary Administrator

User ID	admin
Password	**********
Confirm Password	**********

Setting up Monitoring and Backups

Syslog

Next we move on to the Services -> Syslog section of the Contivity. Here we configure an external Syslog server and the logging level to be sent to it. Remember the Contivity switch carries an internal Syslog as well.

Line	Enabled	Host Name or IP Address	Message Level	Facility	UDP Port
1	☑	192.168.1.2	All	LOCAL4	514
2	☐		Normal	KERN	514
3	☐		Normal	KERN	514
4	☐		Normal	KERN	514

OK Cancel

SNMP

Under Admin -> SNMP the SNMP Get host monitoring information and configuration is set. Up to three server can be set, and the available MIBS can be enabled or disabled.

SNMP IDENTITY

sysDescr	CES V04_75.100
sysObjectId	01.03.06.01.04.01.2505.1700
sysName	vpn
sysContact	Matthew Hall
sysLocation	DataCenter

SNMP-GET HOST

Enable	Host Name or IP Address	Community Name	Status
1 ☑			Operational

2 ☑			Unavailable
3 ☑			Operational

MIBs

Enable	MIB Name	Description
☑	IP Tunnel	(RFC2667) Tunnel statistics
☑	RIPv2	(RFC1724) RIPv2 statistics
☑	OSPF	OSPF Statistics
☑	VRRP	VRRP Statistics
☑	IPX	IPX Statistics
☑	RIPSAP	RIPSAP Statistics
☑	DSU/CSU	DSU/CSU Configuration and Statistics

To setup SNMP traps, navigate to the Admin -> SNMP TRAPS menu. Up to three trap hosts can be configured and individual traps can be enabled or disabled. In addition, the frequency of traps and single send options are available for customization.

Trap Hosts

Enable	Host Name or IP Address	Community Name	Status
1 ☑			Unavailable
2 ☐			
3 ☐			

Trap Groups

Group	Name	Condition	Description	Last Time Sent	Action

Hardware	Heart Beat	OK		05/02/2004 21:39:04	Configure
Server					Configure
Service					Configure
Standard IETF					Configure
Attack					Configure

All SNMP MIBS for the Contivity are included with each software release, and can be compiled using any SNMP v2 compatible compiler.

Backups

The Admin -> Auto backup menu allows for automatic backups of the system. Up to three backup servers can be set for redundancy. It is unadvisable to backup the system files as they can always be restored via a software install on the replacement Contivity in the case of hardware failure. This combined with the fact that the OS image on the Contivity can be up to 150 MB, it is far easier to simply backup the Configuration Files. Log files can be avoided as well if you are already using an external Syslog server for redundancy.

Enabled	Host	Path	Status	Specific time	Interval (hours)	User ID	Password	Confirm Password
1 ☑			Success	○ 05:09:51	◉ 5	ftpbackup	**********	**********
Backup Days	S ☑ M ☑ T ☑ W ☑ T ☑ F ☑ S ☑							
Backup Types	○ Full Backup ◉ Partial Backup			**Partial Backup Configuration** ☐ System Files ☑ Configuration Files ☐ Log Files				
2 ☐				○ 05:09:51	◉ 5			
Backup Days	S ☑ M ☑ T ☑ W ☑ T ☑ F ☑ S ☑							
Backup Types	◉ Full Backup			**Partial Backup Configuration**				

	Partial Backup	System Files Configuration Files Log Files
3		05:09:51 5
Backup Days	S M T W T F S	
Backup Types	Full Backup Partial Backup	**Partial Backup Configuration** System Files Configuration Files Log Files

Up to three backup servers can be specified, including options for login and password, path, time and day of the week. In addition, an option is provided to initiate a backup at set time intervals. Ftp is used for the automated backups, and a secure server should be setup for the service, preferably using IPSEC for encryption.

Routing/Qos Configuration

Routing

Under Routing -> OSPF the options for system wide OSPF configuration are listed. Area IDs and advertised subnets for those areas are configured in this section, as well as LSA types. At the bottom of the screen are several reporting buttons to show the status of the Link State Database, Neighbors and OSPF interfaces on the Contivity.

OSPF

Enabled	Router ID 192.168.1.2	
AS-Boundary-Router False	Auto Virtual Link False	External Metric Type Type1

OK Cancel

Equal Cost MultiPath

OSPF Maximum Paths 1

OK	Cancel

Known OSPF Areas

Area ID	Actions
0.0.0.0	Edit
Add	

Configured Physical Interfaces

IP Address	Area ID	Type	State

Save LSDB Table

Directory /ide0/system/routing	
Filename	
Save	

Status

LSDB	Neighbor	Interfaces (Displays all of the interfaces)	Summary	Statistics

When adding a branch office that you wish to advertise a default route into, we chose to use stub areas. Below is an example of the configuration for a new stub area. We chose the False option for importing summaries, which will result in only a default route being advertised into the area, and no additional routes.

OSPF Area

Area ID	1.1.1.1 (Enter Area ID in IP address format)
Stub	True
Stub Metric	1

Import Summaries	False

The Routing -> interfaces section allows us to configure OSPF interface specific Data. This is where the Contivity is configured to interact with the preexisting OSPF infrastructure and set the md5 keys. Only physical interfaces are configured here. OSPF over branch office tunnels is configured under the tunnel profile and will be covered shortly.

Interface	LAN
IP Address	192.168.1.3
State	Enabled
Area ID	0.0.0.0 Add an Area ID
Type	Broadcast
Authentication	MD5 Key ID 1 Key Confirm Key
Cost	10
Priority	1
Hello Interval	10 seconds
Dead Interval	40 seconds (Dead Interval value must be at least 4 times Hello Interval)
Retransmission Interval	5 seconds
Transmission Delay	1 seconds

It is worth noting that the Contivity only accepts Area IDs in the IP address form. Make sure that the preexisting infrastructure is configured using this format in order to ensure compatibility. Make sure that not only your key, but your Key ID matches the rest of the infrastructure as well.

The Routing -> Configuration menu allows you to set the preferred default route. We will be setting it to “Private” in order to force all traffic across the tunnel. OSPF equal cost load balancing is configured in this section as well, and can be used not only to route traffic back into the infrastructure across equal cost links, but also to route across any equal cost IPSEC tunnels you may have in place.

Equal Cost MultiPath

Maximum Paths	1
OSPF Maximum Paths	1
Forwarding Algorithm	per-destination

Source Interfaces	Outbound Routing Preference
Private	Public (0.0.0.0/32) Private (0.0.0.0/0)

OK Cancel

Qos

The QOS -> Bandwidth MGMT and QOS -> Bandwidth Rates menus are used to enable the internal bandwidth management and set rates for interfaces. These can then be applied to IPSEC tunnels. Several preconfigured rates are provided, but custom rates can be configured as well.

Bandwidth Management	Disabled
Admission Control	Disabled

OK Cancel

Current Bandwidth Rates

- 14.4 Kbps
- 28.8 Kbps
- 56 Kbps
- 128 Kbps
- 256 Kbps
- 512 Kbps
- 1 Mbps
- 5 Mbps

Under the QOS menu, there are also options for setting RSVP and DSCP for further QOS, but that is beyond the scope of this case study.

Tunnel Configuration

Tunnel configuration is formed in two parts for both user and branch office type tunnels. User tunnels are configured in groups and subgroups for all policy and encryption enforcement settings and through individual user account setup using radius or an internal LDAP database under which specific administrative rights and authentication credentials can be assigned. The group structure allows policies to be applied to subgroups by default and overrides to be placed at any level in the tree hierarchy. This allows for the ability to be both granular in policy and to apply policies system wide with a single configuration change. Branch office tunnels are configured in the same group hierarchy as well, with individual tunnel profiles instead of individual user accounts. It is under the tunnel profile section that static routes, preshared keys, and any dynamic routing information and NAT for the tunnels are configured.

User Tunnels

User tunnels are aggressive mode and thus do not verify source IP address but instead use username and password authentication. An additional layer of authentication can be provided with the use of group IDs and passwords that are assigned to individual groups. In addition, these can be used to assign radius authenticated users to a specific security group.

Under the Profiles -> Groups section of the Contivity there are two sections of interest for this implementation. The first deals with client specific settings and policy enforcement and the second with IPSEC specific settings.

Current Configuration Connectivity

Contact Information: None
Access Hours: Anytime
Call Admission Priority: Highest Priority
Forwarding Priority: Low Priority
Number of Logins: 2
Password Management: Disabled
- Maximum Password Age: 30
- Minimum Password Length: 6
- Alpha-Numeric Password Required: Disabled
Static Addresses: Enabled
Idle Timeout: 00:15:00
Maximum number of login attempts to lock out an account.: Disabled
Filters: permit all
IPX: Disabled
Maximum Number PPP Links: 2
RSVP: Disabled
RSVP: Token Bucket Depth: 3000 Bytes
RSVP: Token Bucket Rate: 28 Kbps
User IP Address Source: Default
Address Pool Name: Main Pool
User Bandwidth Policy:
- Committed Rate: 56 Kbps
- Excess Rate: 128 Kbps
- Excess Action: Mark

IPsec

Split Tunneling: Disabled
Split Tunnel Networks: (None)
IPSec Idle Timeout Reset on Outbound Traffic: Enabled
Client Selection:
- Allowed Clients: Only Contivity Client
- Allow undefined networks for non-Contivity clients: Disabled
Database Authentication (LDAP):
- User Name and Password: Enabled
- RSA Digital Signature: Enabled
Default Server Certificate: (None)
RADIUS Authentication:

- User Name and Password: Disabled
- Default Radius Server: Enabled
Server(s): Primary ...
Encryption:
- ESP - Triple DES with SHA1 Integrity: Disabled
- ESP - Triple DES with MD5 Integrity: Disabled
- ESP - 56-bit DES with SHA1 Integrity: Disabled
- ESP - 56-bit DES with MD5 Integrity: Enabled
IKE Encryption and Diffie-Hellman Group: 56-bit DES with Group 1 (768-bit prime)
Accept ISAKMP Initial Contact Payload: Disabled
Perfect Forward Secrecy: Enabled
Forced Logoff: 00:00:00
Client Auto Connect: Disabled
Banner: (None)
Display Banner: Disabled
Keepalive: Enabled
Interval (hh:mm:ss): 00:01:00
Max Number of Retransmissions: 3
Anti Replay: Enabled
Client Screen Saver Password Required: Disabled
Client Screen Saver Activation Time: 5 Minutes
Allow Password Storage on Client: Disabled
Compression: Enabled
Rekey Timeout: 08:00:00
Rekey Data Count: (None)
Domain Name: northamerica.corporate-domain.net
Primary DNS:
Secondary DNS:
Primary WINS: (None)
Secondary WINS: (None)
Nortel Client Requirements:
- Minimum Version: (None)
Client Policy: (None)
IPsec Transport Mode Connections: Enabled

The following settings will be put into place.

Number of Logins: 2
Password Management: Enabled
- Maximum Password Age: 90
- Minimum Password Length: 8
- Alpha-Numeric Password Required: Enabled
Maximum number of login attempts to lock out an account.: 3
Address Pool Name: (Default Pool)

Split Tunneling: Disabled
Client Selection:
- Allowed Clients: Only Contivity Client
Database Authentication (LDAP):
- User Name and Password: Enabled
- RSA Digital Signature: Disabled
Encryption:
- ESP - Triple DES with SHA1 Integrity: Enabled
- ESP - Triple DES with MD5 Integrity: Disabled
- ESP - 56-bit DES with SHA1 Integrity: Disabled

- ESP - 56-bit DES with MD5 Integrity: Disabled
IKE Encryption and Diffie-Hellman Group: Triple DES with Group 2 (1024-bit prime)
Perfect Forward Secrecy: Enabled
Anti Replay: Enabled

The reasoning behind the settings are as follows: These settings are for administrative logins and thus they should have 24 hour access to the switch. The maximum number of logins will be set to 2 in order to allow for multiple screens to be used by administrative staff. Password management was set in accordance with preexisting corporate policy, and the address pool was set to default, which provides for the use of an external DHCP server. Only the Contivity client is allowed to connect due to it's superior policy enforcement. RSA authentication is disabled since it is not in use. The Cipher strength was discussed earlier in the case study. Perfect forward secrecy and Anti Replay were enabled to provide additional levels of security.

General

	First	Last
Name		
Group	/Base	

	Static IP Address	Static Subnet Mask
Remote User		

Note: The static IP subnet mask is used for IPsec connections only

User Accounts

	User ID	Password	Confirm Password	Expires (Days)	Status
IPsec					
PPTP					
L2TP					
L2F					

Must Change Password at Next Logon	(Nortel IPSEC Client Only)

L2TP/IPsec Data Protection

Require Own IPsec Credentials	

Administration Privileges

	User ID	Password	Confirm Password
Admin			

Admin Rights	Manage Switch	Manage Users	
	None	None	

User accounts are configured under the Profiles -> Users section. Only accounts for Senior Networking staff were created with administrative rights to the switch. Other networking staff accounts were created with view only privileges. All accounts were assigned a password that was delivered via voice communications to each user, and the "Must Change Password at Next Login" option was selected to force a new password to be set upon initial login. This was done to not only insure confidentiality of the user password but also to provide some level of non-repudiation to any auditing that was done. By ensuring that no one knew a user's password, except the user themselves, there was a greater assurance that changes tracked to the users account were indeed performed by the user in question.

Branch Office Configuration

Branch office tunnels can be configured to use Main mode in which the source IP address is verified for additional security, or aggressive mode in the case ABOTs, in which a dynamic IP address is assigned to the public interface of the branch office.

Branch office configuration begins much like user configuration. Policy is set first by editing the group object under which the tunnel will be placed.

Current Configuration Connectivity

Nailed Up: Enabled
Access Hours: Anytime

Call Admission Priority: Highest Priority
Forwarding Priority: Low Priority
Idle Timeout: 00:15:00
Forced Logoff: 00:00:00
RSVP: Disabled
RSVP: Token Bucket Depth: 3000 Bytes
RSVP: Token Bucket Rate: 28 Kbps
Branch Office Bandwidth Policy:
- Committed Rate: 56 Kbps
- Excess Rate: 128 Kbps
- Excess Action: Mark

IPsec

Encryption:
- ESP - AES 128 with SHA1 Integrity: Disabled
- ESP - Triple DES with SHA1 Integrity: Disabled
- ESP - Triple DES with MD5 Integrity: Disabled
- ESP - 56-bit DES with SHA1 Integrity: Disabled
- ESP - 56-bit DES with MD5 Integrity: Disabled

IKE Encryption and Diffie-Hellman Group: AES 128 with Group 5 (1536-bit prime)
Vendor ID: Enabled
Accept Aggressive Mode ISAKMP Initial Contact Payload: Disabled
Perfect Forward Secrecy: Enabled
Compression: Enabled
Rekey Timeout: 08:00:00
Rekey Data Count: (None)
ISAKMP Retransmission Interval: 16
ISAKMP Retransmission Max Attempts: 4
Keepalive interval: 00:01:00
Keepalive (On-Demand connections): DISABLED
Anti Replay: ENABLED

The following settings were used.

Nailed Up: Enabled
Access Hours: Anytime

Encryption:
- ESP - AES 128 with SHA1 Integrity: Enabled
- ESP - Triple DES with SHA1 Integrity: Disabled
- ESP - Triple DES with MD5 Integrity: Disabled
- ESP - 56-bit DES with SHA1 Integrity: Disabled
- ESP - 56-bit DES with MD5 Integrity: Disabled

IKE Encryption and Diffie-Hellman Group: 56-bit DES with Group 1 (768-bit prime)
Vendor ID: Enabled
Accept Aggressive Mode ISAKMP Initial Contact Payload: Disabled
Perfect Forward Secrecy: Enabled
Compression: Enabled
Rekey Timeout: 08:00:00
Rekey Data Count: (None)
ISAKMP Retransmission Interval: 16
ISAKMP Retransmission Max Attempts: 4
Keepalive interval: 00:01:00
Keepalive (On-Demand connections): DISABLED
Anti Replay: ENABLED

OSPF

Priority: 1
Dead Interval: 40
Hello Interval: 10
Retransmission Interval: 5
Transmission Delay: 1
Authentication Type: MD5
- MD5 Password:
- MD5 Key:

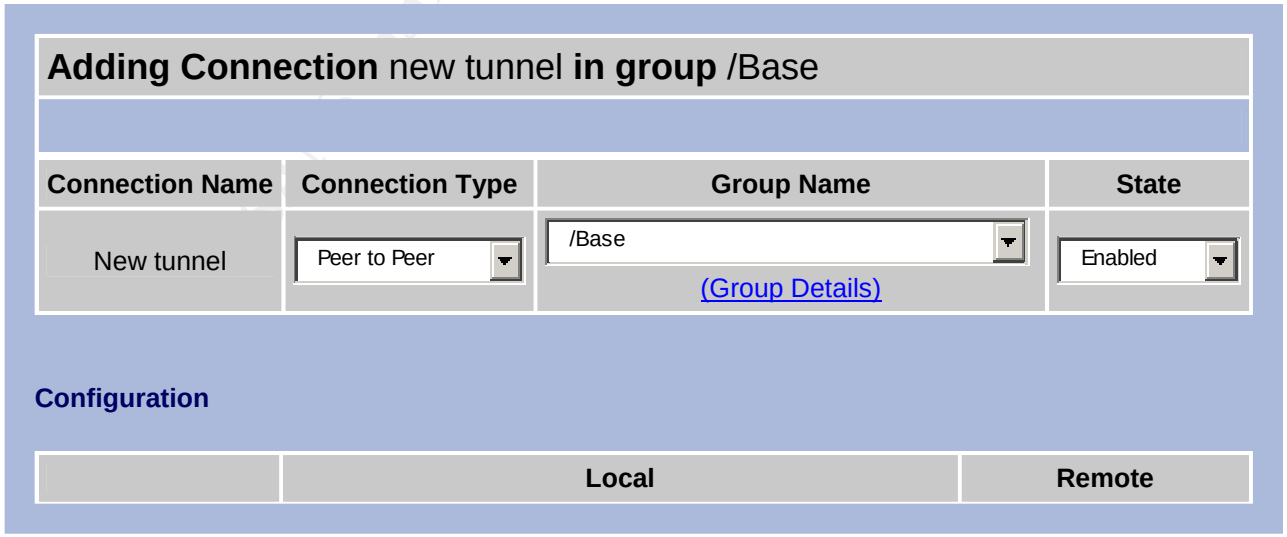
The reasoning behind the settings are as follows: The Nailed Up option was enabled to ensure that tunnels would try and stay established regardless of traffic in order for proper monitoring of tunnel status. Access hours were set to

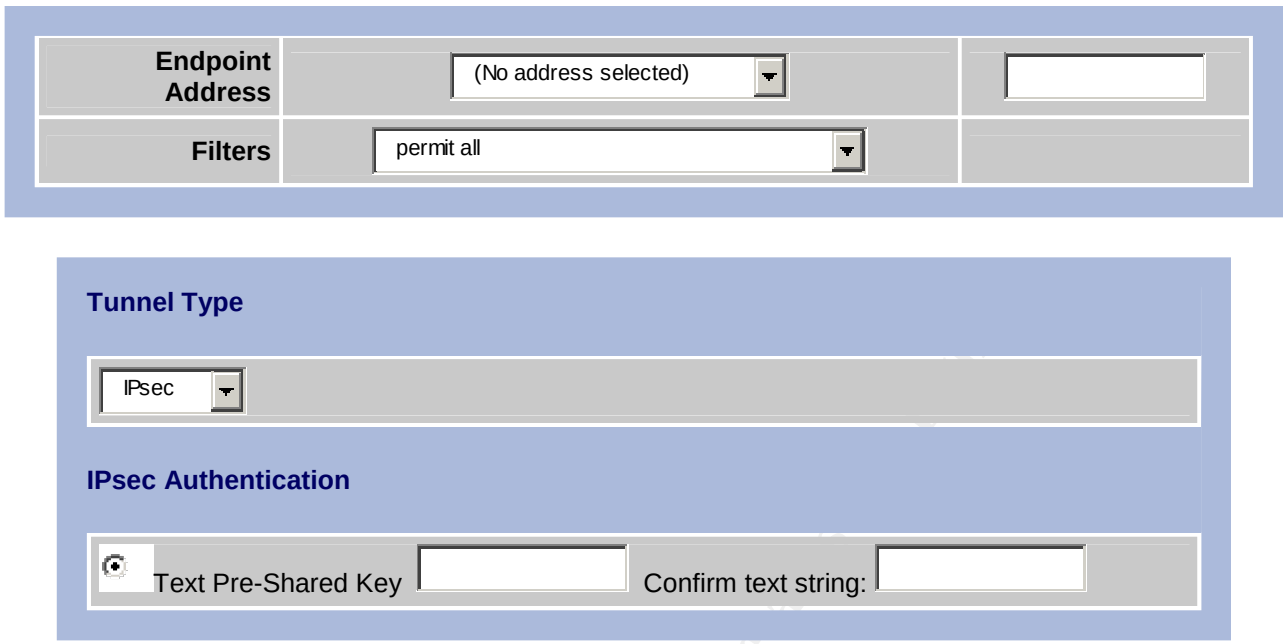
"Anytime" because of commitments to availability that had to be delivered. It is, however, advisable to try and limit these to business hours for remote branches if feasible, in order to ensure proper business use of network resources. Bandwidth policy on each tunnel was set differently depending on the business need of each office in order to assure QOS was delivered judiciously. Ciphers in user were discussed above, and only the required ciphers were enabled to ensure proper negotiation of the tunnels. Other security based settings were set for similar reasons listed under the user tunnels explanation section above. The "Rekey Timeout" setting was maintained at 8 hours due to the currently secure nature of AES 128 encryption. It was thought that currently no entity could feasibly decrypt the key in the set amount of time without a cost in excess of that required to purchase the organization itself. Finally, OSPF settings were put into place to match those of the existing corporate infrastructure.

Main Mode tunnels

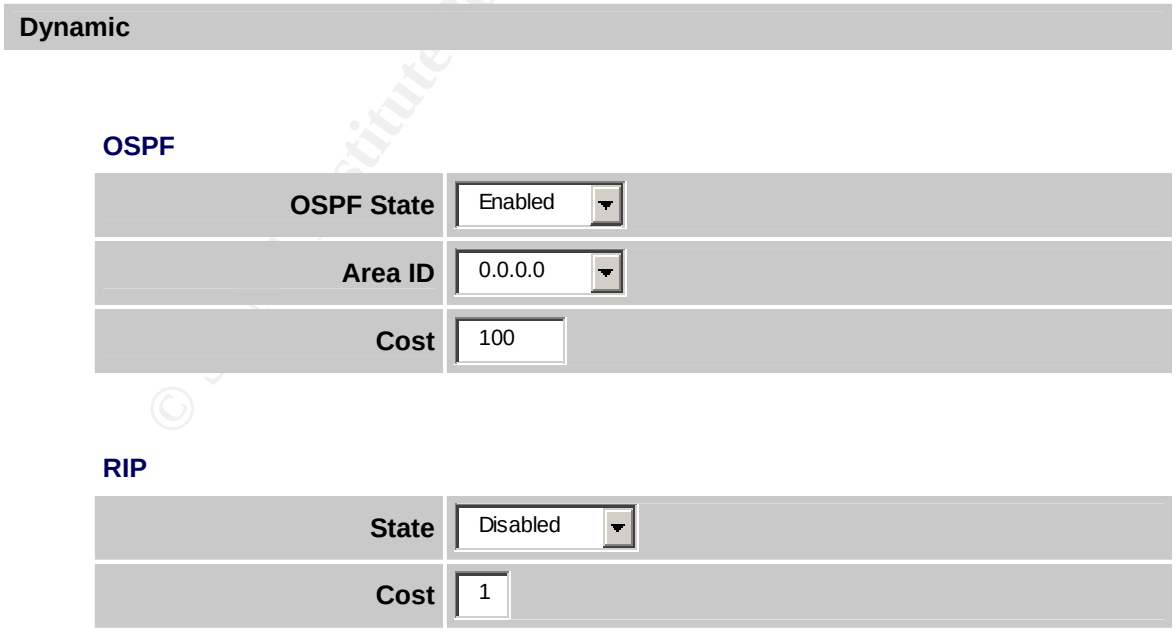
To define an individual tunnel under a specific policy, click the "Define Branch Office Connection" button under the Profiles -> Branch Office section of the configuration. Apply a name to the tunnel. For Main Mode tunnels select "Peer to Peer" from the connection type in the dropdown menu. Then select the group policy you wish to place the tunnel under. Click the "OK" button to continue.

Now select enabled for the tunnel status. Under the "Local and Remote Endpoint Address" section select the local IP address of the Contivity under the "Local" column and type the external IP of the remote branch office Contivity into the "Remote" column. In the tunnel type section, choose IPSEC. Under "IPSEC Authentication", type your preshared key into the text-preshared key and confirm preshared key boxes. Be sure the radio button next to this option is selected as well.



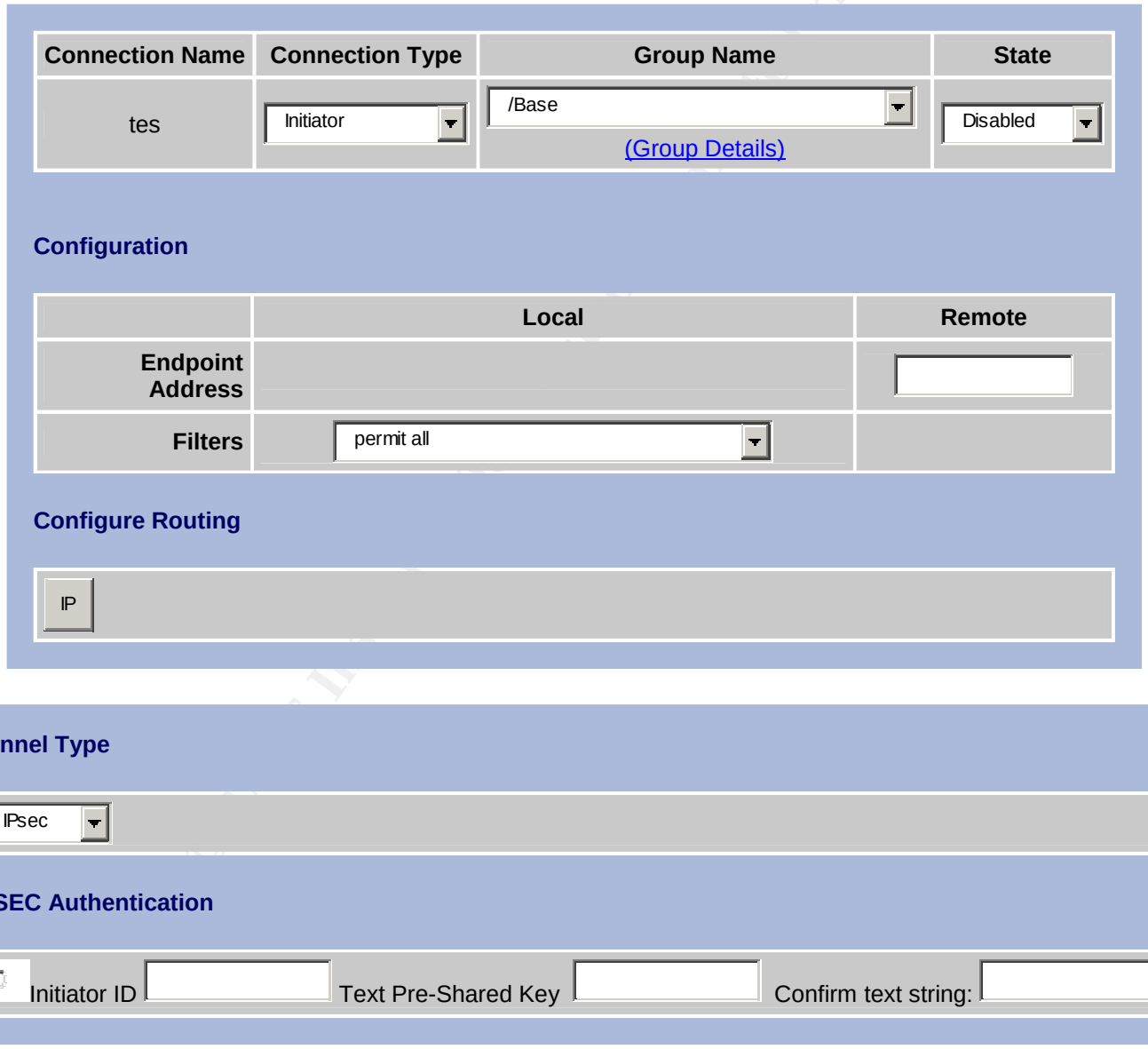


Click the IP button under the “Configure Routing” section. Select the Dynamic radio button and choose “Enabled” under the “OSPF State” section, and “Disabled” under the “RIP State” section. Select the proper area ID from the drop down menu, and apply the appropriate cost to the link. Click the “OK” button to accept the changes and exit to the previous screen, where you will click “OK” again to apply the settings.



ABOT (aggressive mode tunnels)

Configuration of aggressive mode tunnels is identical to that of main mode except for a few steps. Under the “Connection Type” drop down, choose “Initiator” on the device that will be assigned a dynamic IP address and “Responder” on the device that is on the opposite side of the tunnel. In addition, there will be an “Initiator ID” box to fill in next to the text-preshared and confirm preshared key boxes that must be the same on both devices. This is used to add an additional layer of security to the aggressive mode tunnel, since aggressive mode tunnels do not verify the source IP address of the incoming IKE negotiation.



Connection Name	Connection Type	Group Name	State
tes1	Responder	/Base (Group Details)	Disabled

Configuration

	Local	Remote
Filters	permit all	

Configure Routing

IP

Tunnel Type

IPsec

IPSEC Authentication

Initiator ID | Text Pre-Shared Key | Confirm text string:

VRRP configuration

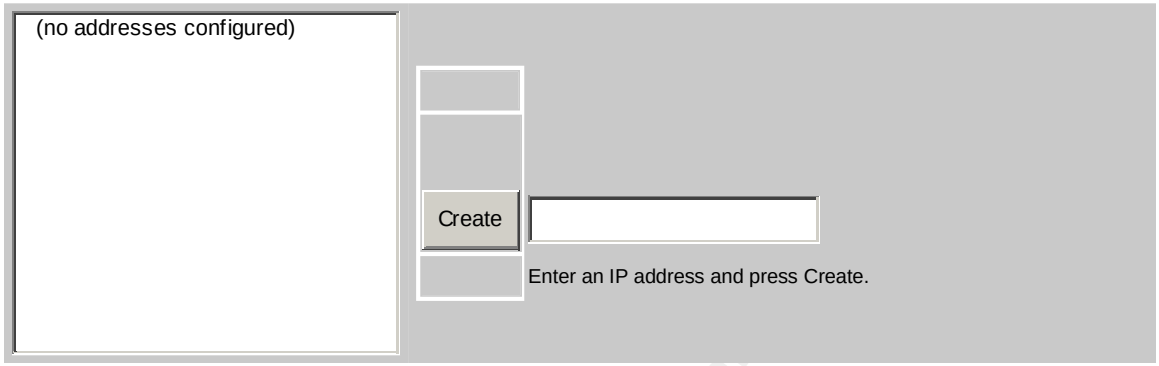
Creating The Shared Address

One the primary device, under the Routing -> VRRP section of the menu, put the shared address in the “Create” box and press the “Create” button.

VRRP

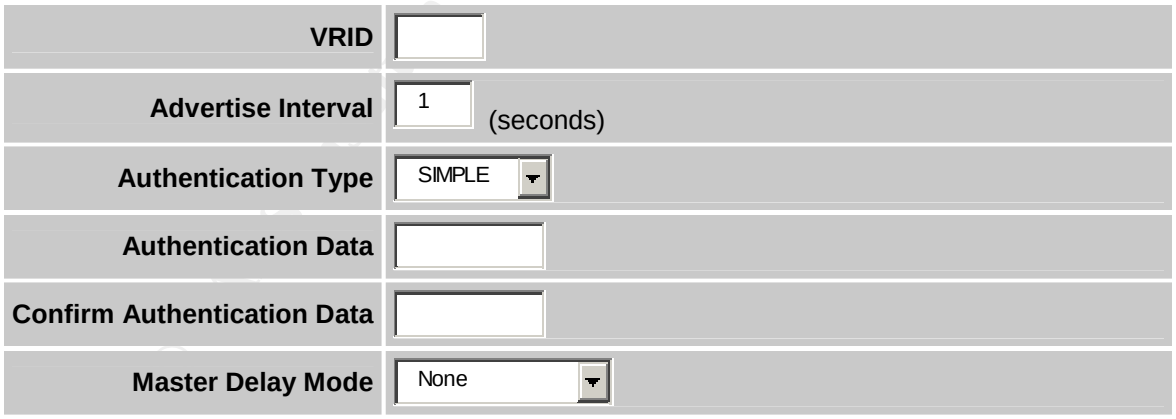
Enabled

Addresses Configured for VRRP



Configure a VRID for the shared IP address, and choose simple under the authentication type. Enter a key into the authentication data sections. This key will be used to prevent unintentional errors in VRRP operation due to a "rouge" node on the broadcast domain but provides no real security, due to the fact that it is unencrypted. Press the "OK" button to return to the main menu. Select the Enabled check mark, and click "OK".

Create 192.168.1.1

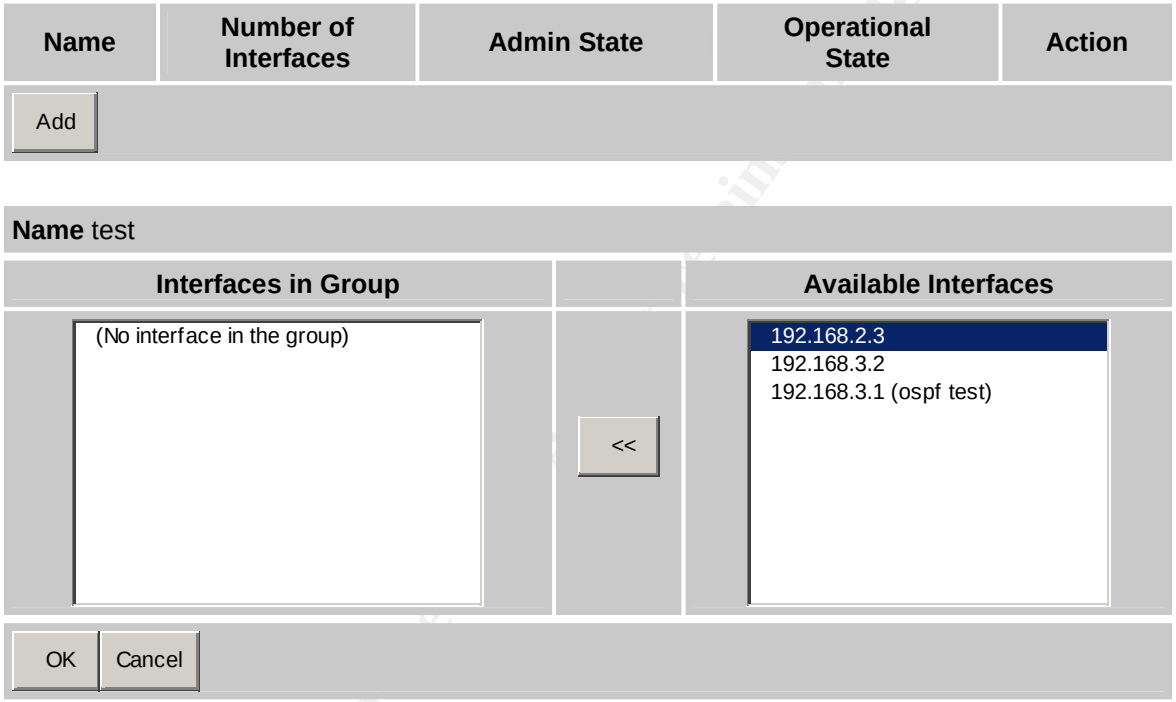


Tunnel Groups

Normally, VRRP will only failover if the two interfaces sharing the address loose contact with each other. If a remote tunnel or public interface goes down, and the hardware devices are both still active on the private side, then the VRRP address will not fail over, and traffic will be routed to the wrong device! In order for the VRRP address to failover, it must have accurate monitoring of the VPN tunnels.

Since the loss of one tunnel or interface is not always a sufficient indicator for failover, Nortel provides for tunnel/interface groups to be configured. In this case, an entire group of tunnels and or interfaces must fail before failover will occur.

Under the Routing -> Interface GRP section of the Contivity, click the “Add” button. Type a name into the Name section, and choose tunnels or interfaces from the right box of available resources and move them into the interface group by pressing the button marked “<<”. When you are finished, press “OK”. In this case we will be adding all branch office tunnels.



As stated above, in order for failover to occur, all members of the group must fail. Up to three groups can be associated with a VRRP instance. If any single group fails, then the VRRP address will fail over. For this reason, it is advisable to create two groups. One group contains the public, physical interface; the other contains the IPsec tunnels. That way if all of the tunnels go down but the physical interface stays up, the VRRP address will still fail-over.

VRRP Completion

The final step of configuration is to navigate to the VRRP section of the Routing -> Interfaces menu. In this section, you will need to click enable for the interface sharing the IP address. In addition, you will need to click “Serve as Master” next to the VIRD being shared. Then select any interface groups that you want to be associated with the VRRP address and click “OK”.

Master Status

Serve as Master	VRID	Operational State	Critical Interface
☑	4	Master	

Group	Interface Group	Enabled (Administrative State)	State (Operational State)
Group 1	test	☑	UP
Group 2	None	☐	UP
Group 3	None	☐	UP
	Interface Group		

OK Cancel

Configuration on backup devices is identical, except for the fact that you will not need to create interface groups and you must choose the appropriate VIRD from a drop down box in the “Backed Up Address field” rather than selecting “Serve As Master”. The default priority in place will be fine for a two gateway setup.

Current Backed up Addresses

Backed Up Address	VRID	Configured State	Operational State	Priority	Actions

New Backed up Address

Backed Up Address	
Priority	100

Add

Current Backed up Addresses

Backed Up Address	VRID	Configured State	Operational State	Priority	Actions
192.168.2.3	4	Enabled	Backup	100	Edit Delete

New Backed up Address

Post Deployment Problems And Solutions

Deployment Problems

It was discovered very early on that only a few infected users at one site could affectively use all of the bandwidth for a branch office link. This would cause a denial of service attack at the location. Quality of service did not provide an affective solution, due to the fact that it could not be granular enough with the classifications to sort any future legitimate data traffic from the illegitimate. Voice however could be protected as always. The solution was yet another example of defense in depth. Multiple layers of protection and detection were added. The IDS at the main office was tuned to discover DOS and Port Scan hosts and notify us immediately via SNMP. This allowed for early detection of the questionable traffic. NetFlow caches on the main office core routers were consulted to verify the nature of the traffic, and the stateful firewall at the branch location was then used to drop the offending traffic until the system could be sanitized. In addition, compliance with the new virus scanning software was enforced using centralized software and local desktop support surveys of systems. Each approach came together to provide for risk mitigation to an otherwise difficult problem.

The stateful firewall itself did show some unexpected behavior and it is worth noting to anyone deploying with the V4_75.100 code version (and perhaps others).

1. Destination LAN interface rules have no affect on branch office sourced traffic.
2. A Destination LAN interface filter set to allow all can nullify any blocking done from source based user tunnel filters for traffic arriving from that user tunnel.
3. Similarly a Destination user tunnel filter can nullify any source based LAN interface filters for traffic destined for the user tunnel.
4. Destination LAN filters seem to only affect non-tunnel traffic that is originating from the Contivity itself (OSPF announcements, etc.). They seem to have no affect on LAN to LAN traffic.

In some cases the firewall seemed to ignore the above stated rules. Due to nature of the stateful firewall, it is advised that all firewall rules be fully tested in either a lab environment or during an outage window.

It was discovered that VRRP failover would sever connectivity to the management IP address of the master. This could be solved in two ways. The first was simply to let it go. The devices could be contacted with the VPNient via the public interface, at which point troubleshooting could occur, or through the use of out of band management. The second option was to forgo the use of tunnel groups and simply setup both devices with a "virtual" IPhat neither system owned. Using priority, one device was set as a primary and the second a backup. If a public interface or tunnels went down, OSPF would route traffic between the private interfaces of the devices, assuring traffic was delivered to its destination. Without an owner for the VRRP address, the address will not be reachable via ICMP for monitoring. Both system's actual IP addresses and management addresses will be reachable and there is a SNMP trap that will be sent in the case of a VRRP failover event.

Monitoring

Proper monitoring is essential in the ongoing security of the system. As mentioned above,the system is still vulnerable to internal DOS, as well as accidental and malicious OSPF route injection. This system must be monitored for brute force password compromise attempts as well. All of this should be done with the use of a centralized SNMP and Syslog server. Above,we setup the Contivities to report back using Syslog and SNMP services, simple base lining and alerting functions now need to be setup on your monitoring solution, which is beyond the scope of this document.

Staying Current

It is highly advisable to subscribe to Nortel's product alert and software update email groups. This can be done at http://www.nortelnetworks.com[5], but requires a current support contract to do so. In addition, there are many other public lists that can be subscribed to in order to stay on top of vulnerabilities. These can be used to build custom fingerprints for you IDS as well as firewall filters in advance of any infection.

CERT Coordination Center[6]:
http://www.cert.org/nav/index_red.html

[5] Nortel Networks Limited. 1999 – 2004 URL: http://www.nortelnetworks.com (11 June 2004)
[6] CERT Coordination Center: "Advisory Mailing List" CERT Coordination Center. 2004. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.
URL: http://www.cert.org/nav/index_red.html (11 June 2004)
URL:http://www.cert.org/contact_cert/certmaillist.html (11 June 2004)

http://www.cert.org/contact_cert/certmaillist.html

Neohapsis Security Threat Watch[7]:
http://www.nwc.com/stw/
http://66.37.227.73/BTG/NLS/yns.asp?K=SANS1016&Q=56

[7] CMP Media LLC. And Neohapsis "Neohapsis Security Threat Watch." TechWeb. 2004. URL:http://www.nwc.com/stw/ (11 June 2004)
URL: http://66.37.227.73/BTG/NLS/yns.asp?K=SANS1016&Q=56 (11 June 2004)

References:

[1] Cisco Systems, Inc. “Cisco IOS Software NetFlow.” 1992 – 2004. URL:http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml (11 June 2004)

[1] Chan, Jason. “Secure Routing?!?” Securing OSPF. February 2001. URL: http://www.liquifried.com/docs/security/securingospf.html (11 June 2004)

[1] Alcatel. “Key Management and Exchange.” Understanding the IPSec Protocol Suite. 2001.
URL:http://www.cid.alcatel.com/doctypes/technewbridgenote/pdf/ipsec_nn.pdf;$sessionid$BM1G5FQAABCKPQCLC3GHBM2KPBUSQ2G0 (11 June 2004)

[1] RSA Security. “What is the AES?” Techniques in Cryptography. 2003.
URL:http://www.rsasecurity.com/rsalabs/node.asp?id=2235 (11 June 2004)

CERT Coordination Center: “Advisory Mailing List” CERT Coordination Center. 2004.
CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.
URL: http://www.cert.org/nav/index_red.html (11 June 2004)
URL:http://www.cert.org/contact_cert/certmaillist.html (11 June 2004)

CMP Media LLC. And Neohapsis “Neohapsis Security Threat Watch.” TechWeb. 2004.
URL:http://www.nwc.com/stw/ (11 June 2004)
URL: http://66.37.227.73/BTG/NLS/yns.asp?K=SANS1016&Q=56 (11 June 2004)

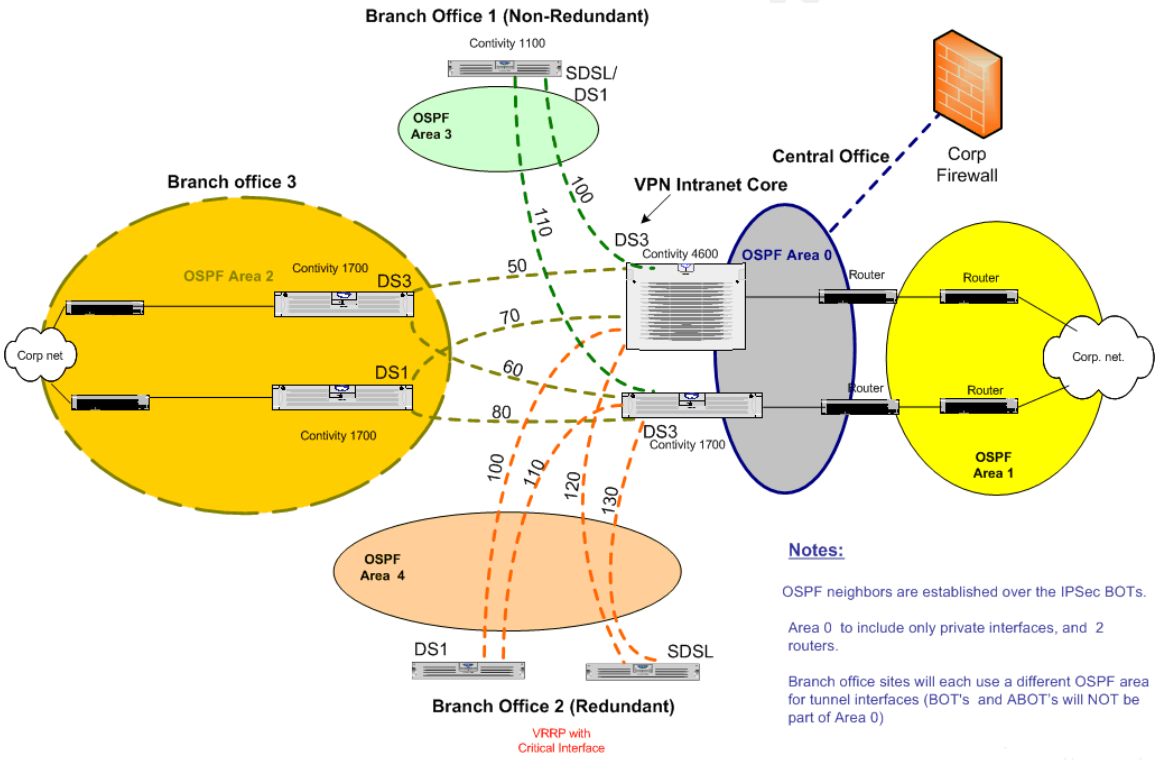
Nortel Networks Limited. 1999 – 2004 URL: http://www.nortelnetworks.com (11 June 2004)

Rijmen, Vincent. “The block cipher Rijndael” 2004.
URL: http://www.esat.kuleuven.ac.be/~rijmen/rijndael/ (11 June 2004)

Nortel Contivity Technical Documentation:

Nortel Networks Limited. 1999 – 2004 URL: http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=documentation (11 June 2004) (Direct Linking to Documents is not possible on Nortel’s Web Site, but they are publicly accessable.)

Below is a layout of the finished deployment. It has been abbreviated using examples of different branch office layouts, in the interest of space and granularity.



Last Updated: October 17th, 2017

Upcoming Training

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