

**NetCo Security System Response**

**by**

**Ryan Moore**

**This paper is being submitted as fulfillment of the requirements for MGT 7382**

**University of Dallas**

**Graduate School of Management**

**John South**

**Fall 2005**

**11/11/2005**

# Table of Contents

Executive Summary .....	1
Business Requirements .....	1
Risk Assessment.....	2
No Security Policy in Place .....	3
Internal Network and Core server are directly accessible from the Internet .....	3
All Applications and Data reside on the same server .....	3
FTP Server.....	4
Web Sever Security.....	4
No set Rules for Passwords .....	4
Protection from Malicious Code .....	5
Network Segregation.....	5
Remote Access .....	6
Third Party Connections.....	6
Wireless Network Security .....	6
Insecure Operating Systems .....	7
Patch Management .....	8
External Email Systems .....	8
Instant Messaging .....	8
Business Contingency and Disaster Recovery Planning.....	9
Physical Security Risks .....	9
Cryptography.....	10
Operational Security.....	10
Intrusion Detection and Incident Response.....	10
Security Policy.....	11
Enforcement and Compliance .....	12
Acceptable Use Policy.....	13
Network Connectivity Policy .....	15
Information Sensitivity Policy.....	17
Operations Security.....	18
Network Devices Policy.....	20
Privacy Policy .....	22
Business Continuity Planning and Disaster Recovery Policy .....	22
Physical Security .....	24
Awareness Training Policy .....	24
Security Solution System Description.....	25
Netco WAN .....	26
Dallas HQ Network.....	28
IP Address Plan .....	29
HQ Network Domains.....	30
Internet DMZ .....	35
Remote Offices .....	38
Summary.....	39

## **Executive Summary**

This document has been prepared in response to Netco's request for a proposal to address the security needs of their network. Netco has made the right decision by taking the necessary steps to improve their security. Penetrating computer networks is no longer the realm of "kids" or "hackers" breaking into systems for fun. Professional Computer Criminals use sophisticated attack methods to steal valuable corporate data and sell it to competitors. Problems resulting from insufficient network security have already arisen at Netco. Netco competitors appear to be using designs based on Netco design data. This has resulted in a loss of Market share. The goal of this proposal is to provide a "defense in depth" security system designed to protect Netco's assets. To meet this objective the following details are included:

- An Enumeration of the Business Goals of the Netco Network
- A Risk Assessment of the current network security problems
- An Outline of a Security policy that addresses the Risk Assessment
- A formal Network Security Design detailing technology options to achieve the goals laid out in the Security policy

## **Business Requirements**

Security is often considered a detriment to business. It is seen as a "necessary evil" that protects corporate assets at the expense of business goals. This could not be further from the truth. A core Axiom of security design is "*Business is the first priority.*" A good security system serves the business goals rather than hampers them. The

business requirements drive the entire design process. The following business goals have been gathered from the information provided:

- Sensitive Information such as Fabrication plans, Design Data , and Financial Records must be protected
- Netco Employees must be able to communicate using Email and share files.
- Netco Employees must be able to use Network Resources such as Databases
- The core offices located in Dallas, Shanghai, and Brussels must have network connectivity to each other
- Engineering and Sales need remote access to the network
- Third parties such as the Fabrication Facility need to be able to communicate with Netco and share files.

## **Risk Assessment**

A risk assessment is an analysis of the potential risks to a company's assets. The analysis of the risks combined with the business goals drives the creation of the security policy and ultimately the design of the security system. This does not constitute a complete risk assessment of Netco. In order to perform a complete risk assessment a comprehensive list of all Netco's assets would first be created. The assets would be evaluated to determine what threats are present for each asset. The information below summarizes a preliminary risk assessment done from the information provided about the Netco network.

### **No Security Policy in Place**

A security policy defines the rules by which people who have access to Netco's network must abide. A written security policy provides the rules for how the network is designed, operated, and used on a daily basis. Without a security policy in place, the design of the network is haphazard and can result in security problems. The next Section of the proposal provides an outline for the Netco security policy.

### **Internal Network and Core server are directly accessible from the Internet**

This represents a very high risk to the security of the network. The Netco internal network and core server can be accessed directly from the internet. Anyone who has access to the internet can access the Netco network remotely. This network contains Netco's most valuable information assets. From the internet an attacker can easily browse Netco's network and look for ways to further attack the system. An attacker can also attempt access Netco's server and steal valuable information. A denial of service attack could also be mounted against the Netco network denying Netco Employees access to network resources. Having the network open to the internet makes it more susceptible to attack from Viruses, Worms and Trojan horse programs. Access to and from the internet into Netco should be controlled and monitored.

### **All Applications and Data reside on the same server**

The Netco server houses all applications and data. The FTP server, Web Server, and Database server are all located on the same server. This is a high security risk as it allows an attacker to concentrate on a single target. Once the server has been compromised, an attacker has access to all of the Netco's sensitive information.

In this configuration, access to data within cannot easily be controlled. The Sales employees do not need to have direct access to Netco's design data. Sensitive data

such as financial records and equipment designs should be placed on separate servers so access can be controlled.

### **FTP Server**

Netco's FTP server is accessible from the Internet and does not have a password set. This means that anyone can gain access the FTP server, browse the files, and copy them. This represents one scenario where design data could have been stolen, as the Fabrication plant uses the FTP server to transmit fabrication designs.

### **Web Sever Security**

Netco's web server resides on the same server as all of Netco's applications and data. Netco's Web server, by necessity, must be accessible from the internet. It doesn't do much good to have a corporate webpage if no one can see it. Special security precautions must be taken in order to insure that Netco's webpage can be seen and used from the internet but does not pose a threat to network security.

The web pages that reside on the server were not professionally designed. The student who wrote the pages may not have been skilled in how to create secure web applications. Unintentional vulnerabilities may exist on the netco web server that need to be addressed.

### **No set Rules for Passwords**

Passwords are an important part of network security. At a basic level they provide access control and authorization to use network resources.

Most network systems transmit passwords from the client to the server in an encrypted form and encrypt all stored passwords. Establishing rules for password creation will prevent them from being stolen and used by an attacker this problem.

In addition to utilizing good passwords that cannot be cracked, passwords should be employed for all network resources. If a network resource does not have a password, an attacker can gain access to the resource directly with little effort.

### **Protection from Malicious Code**

Viruses, Worms, and Trojan Horse programs are rampant on the internet. Simply by being open to the internet Netco's desktop machines and servers may become infected with one of these programs and cause serious problems on the network. Viruses and Worms that infect your network will cause damage to computer systems or tie up the network and make it unavailable for use. An even greater threat is infection by Trojan Horse. A Trojan Horse will allow an attacker to remotely control the infected computer and use it to attack other systems within the Netco network or to launch attacks against other external systems.

### **Network Segregation**

The design of the internal network has been haphazard. There is no formal IP addressing structure and no segregation of the network by function. In the current network, every device on the network has access to every other device. This poses serious risks to the network. An attacker who gains access to the edge of the network effectively has access to the entire network, including remote offices. If a system becomes infected with a virus or worm, it will quickly spread throughout the network infecting more systems.

Dividing the network into separate zones has multiple advantages:

- Access to and from each zone can be controlled
- Traffic internal to the zone stays local, thus preventing sniffing attacks.

- Network performance is increased as the overall network traffic is reduced

### **Remote Access**

Currently, the Netco network can be accessed remotely through the internet as well as through a modem directly connected to the server. Though this makes it easy for Netco's employees to access the network, and work remotely, it also makes it easy for an attacker to gain access to the system.

The modem connected to directly to the server presents an easy opportunity for an attacker to exploit. Computer criminals will often dial every number assigned to a particular company to discover phone numbers that have a computer attached to them. Once the phone number to the modem is known, the attacker can then connect directly to the server and attempt to gain access to it.

### **Third Party Connections**

Connections from third party companies are not controlled. This represents another path that an attacker might utilize to gain access to the Netco network. If the network security of the Third Party is compromised then Netco's security is compromised as well.

There is also no written third party agreement in place. This makes any access from a third party an unknown quantity. If a security breach were to occur as a result of actions taken by a third party Netco would have little legal recourse against them.

### **Wireless Network Security**

An unsecured wireless Access point provides a backdoor into your network. An attacker does not need physical access to your network to connect to it. Anyone in

range of the wireless AP can sign on to the Netco network. Once on the wireless network an attacker has full access to Netco just as if they were directly connected to it.

Close attention must be paid to how Wireless networks are configured and how access is granted. The standard security features and authentication methods that are built into wireless Access Points can easily be defeated and exploited by attackers.

### **Insecure Operating Systems**

The Netco computer systems use a combination of Windows 98 and Windows 2000 for their operating systems. While no operating system available today is completely secure these two Operating Systems are less secure than alternatives that are available.

Windows 98 was developed before security was a large concern in the industry. It is nearly impossible to make a windows 98 desktop machine even reasonably secure. A fully patched and hardened Windows 98 machine is still vulnerable to attack.

Windows 2000 was developed with security in mind but the patches must be kept up to date in order for the system to be secure. Windows 2000 still has a large number of security flaws even when patched fully. Netco would be better served by running a more modern operating system.

One further problem is that the Operating systems in use are all from the same vendor. If critical network devices use different operating systems, it is that much more difficult for a hacker to exploit the vulnerabilities of a single OS.

## **Patch Management**

Patch management is very important in protecting Netco's network. Computer vendors release patches on regular basis to fix security flaws. A system is immune to any attacks that try to exploit a known vulnerability that has already been patched.

New viruses and worms often appear quickly after a new vulnerability is discovered. Automated Patch management and distribution is needed to keep systems from being exploited by new threats.

## **External Email Systems**

Netco's employees all use some form of external email system for communication. Email systems represent a high risk to security. The email system resides out of the control of Netco's IT staff. Many worms and virus are spread through email and it is impossible to provide proper protection if the email services are external. Additionally, there is no way to guarantee that any communication done over external email system is secure. Any sensitive information sent through these systems could be compromised.

Use of external email systems can also pose legal problems for Netco. Email is often considered evidence in court proceedings and Netco could be required to supply copies of past emails. Without an internal email system and a written email retention policy, Netco could be in real trouble in this situation.

## **Instant Messaging**

Instant Messages are an external communication path that cannot be guaranteed to be secure. Instant messaging does not provide client to client communication, even though it may appear that way. All instant messages are routed through a central server and then redistributed. IM clients do not use any form of encryption so the

messages may be intercepted en-route. The file sharing features present in most IM clients can be used by an attacker to infect a computer with malicious code.

### **Business Contingency and Disaster Recovery Planning**

Disaster recovery and Business Contingency planning are a very important part of a security system. Netco does not have any plans in place to recover from a disaster situation. Currently, all of Netco's valuable data is stored on a single server and the backup tapes are kept with the server. If the building were to catch fire or be otherwise destroyed Netco would be in serious trouble and have difficulty conducting business in the future.

The support status of the server is also unknown. A hardware problem on the server, while not catastrophic, could result in days of lost productivity for Netco employees.

### **Physical Security Risks**

Netco's server, network equipment and computer systems are not physically secure. Anyone who has access to the Netco offices can gain physical access to the server. Almost all devices have a "password recovery" procedure that allows the access password to be reset if the device can be accessed physically. An attacker who can gain physical access to a device can defeat most security controls and bypass any passwords.

Access to locations where computer systems are warehoused must also be tightly controlled. Any misplaced or stolen Netco computing equipment could contain sensitive Netco information. A stolen laptop or PC can be used to gain access to the network if it contains dialup numbers and stored passwords.

## **Cryptography**

The use of cryptography is another layer of a defense-in-depth security system.

A properly utilized Cryptography system:

- Ensures transmitted and stored data is only accessed by individuals who are authorized to do so
- Prevents the modification of data by unauthorized persons
- Establishes the validity and origins of transmitted Data
- Prevents an individual from denying that message transmission took place

The Netco laptop that was stolen may have contained sensitive design data. If all design data was stored in an encrypted format, whoever stole the laptop would get little use out of the stored data.

Cryptography should also be employed to secure Netco's Wide Area Network connections and any remote access.

## **Operational Security**

Netco does not have any form of operational security in place. Operational Security is the process by where the day to day operations of the network are done in a secure fashion. The network should operate on the concept of "least privilege." In other words, network users are given the least amount of access possible in order to do their job. If the average user has the same privileges on the server as an administrator then an attacker only has to gain access to a single user account in order to be able to access the entire server.

## **Intrusion Detection and Incident Response**

Computer problems have begun occurring in China and France. These could be the result of a network intrusion by a computer criminal or even the prelude to a larger

attack on the Netco system. Netco has no Intrusion Detection system in place to detect situations like this. Viruses, Worms, Trojan Horse programs and even live attacks by computer criminals all have network “signatures” that can be detected. An Intrusion detection systems or IDS inspects network traffic for attack “signatures” and alerts security personnel.

Netco also has no incident response procedures in place to investigate signs of network intrusion. Each incident needs to be examined to determine its root cause. Steps can then be taken to prevent future occurrences of the security incident.

### **Security Policy**

The security policy defines the rules by which employees, customers, vendors, and other third parties who are given access to Netco’s network must abide. A written security policy that is approved by upper management and regularly enforced is the core of a security system. The policy acts as a guide for the designers and operators of the network and establishes the benchmark by which the design of the security system is judged. Just as a Human Resource Policy defines how a company manages its employees, the security policy defines how to implement and manage it’s network.

A full security policy contains three separate kinds of documents. A *policy* is a rule that must be followed in order to protect the assets of Netco. A *guideline* is a recommended way of implementing a policy based on industry best practices. *Standards* define the baseline for how a particular policy is to be carried out. For example, a policy could state that passwords must be kept confidential and must be strong. The password guidelines would then define what constitutes a weak password and how to create strong passwords. The password standards would then define the

rules for use of passwords, like how often the passwords should be changed and how to keep passwords confidential.

A security policy is often thought of as a large monolithic document that extensively defines the rules of the network. In practice it is better to define a group of smaller policies in separate documents that can easily be updated as business goals and network risks change over time. The following sections outline a security policy that addresses the Risk Assessment.

### **Enforcement and Compliance**

Policies are only effective if they are enforced. There must be real consequences for non-compliance with a policy. Most of the policies will be enforced through the use of technology that is part of the security solution. For example, the network firewalls will keep network users from accessing parts of the network where they are not allowed. Technology can also be used in a passive manner to enforce policies, such as a Network intrusion system looking for attacks taking place on the network. Compliance to policies can also be done through non-technical means. Management walking around the office to verify that employees are following the written policies demonstrates that the company is serious about policy enforcement. Another non-technical means of enforcement is contractually. Employees must sign an agreement stating that they will follow the security policies. This kind of enforcement is especially useful when dealing with third parties. The contract holds them to compliance with Netco's security policies. Regular security audits should also be done to ensure that security policies are followed.

## **Acceptable Use Policy**

The Acceptable Use Policy (AUP) defines what is considered to be acceptable use of computer equipment and what is unacceptable. Inappropriate use of the computer system can result in network attacks, loss of use, and legal issues. The AUP should contain a section that outlines what is expected of each network user. The following is a short list of guidelines for all network users.

- All users must have a network Identity that is tied to them directly and managed by the identity management system.
- All computing equipment and network devices must be secured with a password.
- Passwords should be created in accordance with the Password Standards and Guidelines defined in the Operational Security policy.
- Passwords must be kept confidential
- All computer systems and equipment as well as any information stored on them are the property of Netco and may be subject to monitoring and access by authorized Netco personnel.
- Employees must not perform any activity that is illegal under local, state, federal, or international law while using Netco resources.
- Software that has not been specifically licensed and approved by Netco should not be installed or distributed
- Malicious software such as Viruses, Trojans, and Worms must not be introduced into the network
- Employees must not circumvent access controls in order to gain access a resource or account that they are not allowed to access.

- Performing any attacks upon the network such as Denial of Service, sniffing packets, and spoofing network information is strictly prohibited.

*Internet and Email acceptable use:* Accessing information through internet and exchanging information through Email are the most common uses of a corporate network. Improper internet and email usage can result in loss of reputation, disclosure of sensitive information, and lead to further attacks against the Netco network.

Netco employees should not access the internet directly. Properly configured proxy gateways must be used for all Internet Access. Internet email systems such as Yahoo, Hotmail, and ISP email accounts should not be used for business related communication. Netco Email systems should not be used to distribute unsolicited or junk emails to people who did not specifically request it. Employees should not access or forward through email any of the following:

- Pornography or Adult oriented material
- Information promoting hate groups.
- Copyrighted video, music or other media
- Email hoaxes, chain letters, pyramid schemes, or other “get-rich-quick” schemes.

Enforcement of the AUP is contractual. Each employee should read and sign a copy of the AUP stating that they understand its contents and will abide by the rules it defines. Content management systems and email scanning technology will also be used to technologically enforce the AUP.

## **Network Connectivity Policy**

If the Netco network was completely closed off from all outside networks it would definitely be more secure. However, this is not in alignment with Netco's business goals. Netco employees need to be able to access the internet for research and to communicate with outside partners. Third Parties such as the Netco Fab facility need to be able to exchange email and files with Netco employees. Netco employees also need to be able to access the network remotely in order to be more productive.

In order to control access to and from external networks *domains of trust* must be established. Domains of trust divide the network into segments based on the level of trust. Firewalls should be used to separate and control access between the Domains of Trust. . All Access between the domains must follow the principle of least access, meaning that each employee is given the least amount of access necessary to do their job.

In general, a Lower Level domain of trust is not allowed to access a higher level domain. Any Lower Level accessing a higher level should employ Strong Encryption or Authentication as defined by the *Authentication and Encryption Standards*. All access from a higher level domain to a lower level domain must be controlled and logged as well.

*Internet Connection and Access Policies:* The internet represents a special case of external connectivity. It is the largest external network that Netco will connect to and represents the largest threat to Netco's Security. The *Internet DMZ* network between Netco's internal network and the internet. It is used to control access to and from the internet. All external internet connections including email, web traffic, and remote access must terminate on a server or security device located in the Internet DMZ. All

internal email and web traffic destined for the internet must terminate on a server located on the internal network. This ensures that internal traffic and Internet traffic are separated and controlled. All connections from the internal network to the DMZ must be documented and use secure protocols. All network devices and servers located in the DMZ must be hardened in accordance with the *Network Devices Policy*.

*Third Party Networks:* In order to conduct business Netco must be able to connect its network to external Third Party Networks. These kinds of connections are known as Extranets. While not as insecure as the internet, third party networks reside outside the control of Netco's IT staff and therefore care should be taken when connecting to them.

All Extranet connections must have a valid business case and be approved and documented by the Security Staff. Third Parties must agree to and sign a *Third Party Network Agreement*. The Third party network agreement should include all of the standards and guidelines that the third party must follow in order to connect to Netco.

*Remote Access:* Remote access can generally be accomplished in 2 ways, through remote dial-up by modem, or through the internet by the use of a Virtual Private Network. Any person given remote access to the network must follow the same security Policies and procedures that are relevant to on-site access. All devices such as home PC's used for connecting remotely to the network must follow the same standards and guidelines as company owned equipment. All Remote Access must be strictly controlled through the use of One Time Password Token Devices.

*Wireless Networks:* Wireless networks are inherently insecure. Physical access to wireless network cannot be controlled and therefore must be treated as a completely open network. Wireless networks must be treated in the same manner as the internet

and follow all of the policies defined for connecting to the internet. Wireless networks must be properly secured. Only IT personnel are permitted to set up wireless networks.

Compliance with the Network connectivity policy is enforced through technical means as part of the network security design. Third party network connections will be enforced contractually through the third party network agreement as well.

### **Information Sensitivity Policy**

The information sensitivity policy defines what information can be disclosed to non-employees as well as the sensitivity levels of confidential information. All Business related information at Netco can be divided into two broad categories. *Public Information* is information that can be freely given out to anyone, such as the information available on Netco's Website. *Confidential Information* is all other information. Confidential information is divided into levels of sensitivity. Each sensitivity level must have defined guidelines for how that information is stored, accessed, distributed, and disposed.

*Least sensitive* information includes general corporate information and some technical and personnel information. It can be distributed by normal mail or email to approved recipients.

*More Sensitive* information includes most business, technical, financial, and personnel information. It may be distributed internally through normal means of communication. Any distribution of More Sensitive data outside of Netco should be encrypted or use an encrypted communications channel.

*Most Sensitive* information includes technical, financial, and personnel information important to the success of Netco. Marketing and Trade secrets as well as

computer source code all fall into this category. It is highly recommended that this level of information be stored in an encrypted format and only distributed through encrypted channels.

Access to confidential information should follow the principle of least access. Employees and contractors should be given access to the least amount of confidential information that is required to do their job.

Encryption should be used to enforce the sensitivity policy. This policy should include the standards and guidelines that define the encryption algorithms and parameters.

### **Operations Security**

Operations Security is the day to day tasks of protecting the network. *Production systems* are the network and computer systems vital to the business operations of Netco. All systems that store critical business information and perform necessary business functions are production systems. Security devices and network infrastructure that protect and provide access to the systems are also considered part of the production network.

Production systems should be located in a clean physically controlled environment with uninterruptible power and controlled temperature. These systems should be redundant and checked regularly. All supporting equipment should be monitored by operations personnel.

All access to the production systems must be controlled. This includes physical access as well as access to the systems through the network. The operational security policy should define the access controls for production systems including:

- All access should follow the principle of least privilege.
- All access should be logged and the logs regularly audited
- Rules for who is granted access to the systems
- Defined levels of access for user and administrator accounts and the limits on each level.
- The way in which access is granted to each system both physically
- The standards for the creation of passwords

Production systems should be separate from systems that are used for development and testing. Any changes to the production systems should follow a defined change control procedure. Changes to the production environment must be documented and approved by the proper staff before they are implemented.

All production systems must have their patch levels maintained. A process should be in place to install emergency patches outside of normal change control should the need arise.

Regular vulnerability scans should be done on production systems to find any security weakness before they can be exploited.

A network management system should be used to monitor all production systems and alert operations staff of problems and security vulnerabilities.

Regular backups should be performed of all production systems in accordance with the Disaster Recovery Policy.

*Intrusion Detection:* Intrusion detection systems (IDS) monitor network traffic for specific types of threats such as network scanning, worms, anomalies, and misuse. IDS should

be used to monitor the production network. The operations policy should include standards for the operation of the IDS including:

- Defined response that should be taken when an Intrusion is detected whether manual or automatic
- Guidelines for effectively tuning the IDS so that operators are not overwhelmed with “false positives”
- Procedures for regular audits of IDS Logs

*Incident Response:* When a security incident does occur it needs to be fully investigated. In this way the incident can be prevented in the future. The operations policy should define an Incident Response Team (IRT). The IRT is responsible for investigating any security incidents. They work to contain the incident, control any damage, and prevent the incident from spreading. The IRT should be composed of both technical and non-technical staff. There should be designated contact lists for each company location that the team can use to gather information about an incident. The team should always provide a post mortem report on the incident. Security Policies and procedures can then be updated to prevent the incident from occurring in the future. Compliance to the Operational Security Policy should be enforced as part of regular security audits.

### **Network Devices Policy**

The purpose of the Network devices policy is to define the guidelines and standards by which devices may be connected to Netco’s network. This includes all networking devices such as routers and switches, all computing equipment such as

servers, desktops, and laptops, and all security devices such as firewalls, IDS, and VPN concentrators. In general all devices should follow these guidelines:

- The devices Operating System must be regularly patched to prevent exploitation of security holes.
- Each must have a defined device hardening procedure and this procedure must be performed on the device before it is connected to the network.
- All devices must be protected from attacks by viruses, Trojans, and worms. This can be accomplished through host based virus protection and in-network virus scanning devices.
- All end user devices must run a host based firewall.
- Devices that will regularly be exposed to open networks such the as internet and wireless networks should be protected by a Host Intrusion Detection System.
- All devices to be connected to the Netco network must first be approved by the IT department.

The policy should also include all guidelines and standards used for securing common types of application servers including database, ecommerce, web, and file servers. Any integration of a unique application server should involve the Security Staff so that the hardening requirements can be established.

Compliance with this policy is accomplished through technical means. IDS systems watch for rogue devices being connected to the network. Software update systems are be used to push new patches and virus updates out to all end user devices. Regular penetration testing and vulnerability scans are used to insure that

application servers are secure. Devices that do not comply with this policy can be forcibly disconnected from the network.

### **Privacy Policy**

One of the fundamental security policies is the privacy policy. This policy should state that all information gathered by Netco from customers and web site visitors will be kept confidential and not shared with any third parties. The privacy policy should define what information is gathered from customers, how the information is gathered and how it is used. The privacy policy should be published on Netco's website and include contact information for people wishing to find out what information has been gathered by Netco. Customer information should be considered "more sensitive" and follow the information sensitivity policy.

Regular audits of how customer data is being stored, used, and collected should be done to insure compliance with the privacy policy.

### **Business Continuity Planning and Disaster Recovery Policy**

The *Business Continuity Planning* (BCP) policy protects the Netco enterprise from events that impede normal business operations. BCP is a multi-step process that correlates what is important to Netco's business operations with how Netco conducts its business. Critical business functions must meet minimum operating requirements during times of crisis or after a disaster. The BCP policy must define exactly what is to be protected during a disaster and the goals of Business Continuity Planning process. Though BCP falls within the scope of the IT department, it should encompass Netco's entire enterprise and not just the information systems. BCP consists of two parts: a Business Impact Analysis and a Disaster Recovery Plan.

A *Business Impact Analysis* or BIA is the heart of BCP process. A BIA assesses how the loss of critical systems effects Netco's operations. The BIA defines the boundaries of the Disaster Recovery Plan. It should begin with a detailed inventory of all company assets. It should define the critical capabilities that must be protected. This inventory should be kept up to date at all times. This is done by defining the critical functions of each department and what systems they rely on to perform these functions. Once completed, the BIA provides the requirements for the Disaster Recovery Plan.

The *Disaster Recovery Plan* (DRP) defines the specific strategies used to recover in the event of a disaster. The plan must document the specific actions to recover the system from a full disaster. The DRP can be dived into three phases. The first phase should concentrate on enabling the most critical business functions, as defined by the BIA, as quickly as possible. The second phase should include plans on how to restore full or near full functionality of the system. The third phase of the plan defines how to accomplish full restoration of the system. When writing the DRP it should be assumed that a complete failure has occurred and that a full recovery is necessary.

Data backup is an important part of BCP and the DRP. Proper data backups also fulfill the requirements of protecting production systems as defined by the *Operational Security Policy* and may be needed in the case of an *Incident Response*. This policy should define the guidelines and standards for data backup of all critical systems. It should define:

- What backup processes are used for each system

- How backups are logged.
- The standards for acceptable backup software and hardware
- The Retention and Storage Policy for Backup Media
- A designated off site Storage Facility for Backup Media

Compliance with the BCP policy can be insured through regular audits. The results of the audits should be used to update the BIA and DRP.

### **Physical Security**

The physical security policy defines the overall physical security of Netco facilities. This policy will have some overlap with Operational Security policy as that policy defines the physical security needed for production system. Access to all Netco facilities must be controlled. All outside exits must be secured and a physical access control system such as card readers should be used. Access to sensitive locations within the facilities containing critical infrastructure such as wiring closets should also use an access control systems. The policy should also include all standards and guidelines for electrical power, heating and cooling, and fire suppression systems.

Physical Security should be regularly audited to ensure compliance with the policy. Logs of the access control system should be regularly reviewed to ensure illegal access is not taking place.

### **Awareness Training Policy**

Netco's own employee's can be one of the most effective countermeasures to security threats. They are often the first to notice a security threat and should be properly trained on how to respond to them. A Security Awareness training program should be developed both to inform Netco's employees about how to conform to the

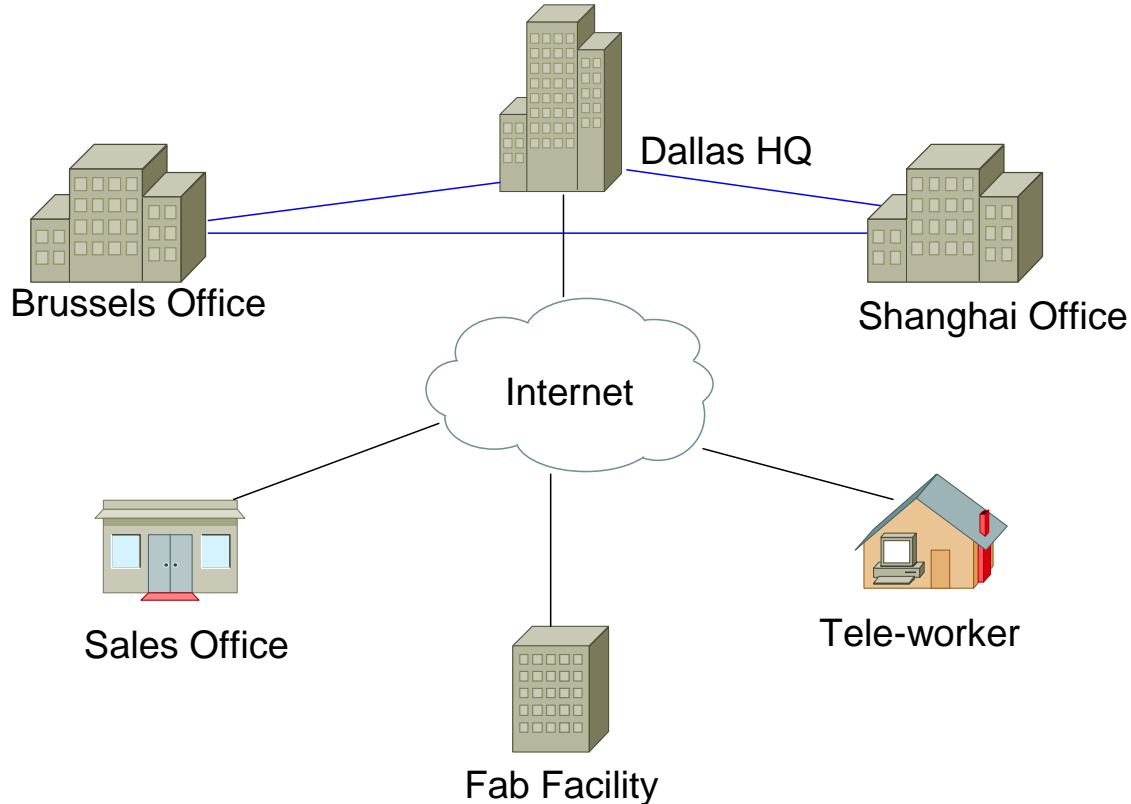
Security Policies as well as how to respond to security incidents. The Policy should state that Awareness training is mandatory. All employees must agree that they understand and will comply with all security policies. The policy should also define who is responsible for providing the awareness training.

The Awareness training program should begin after the Security Policy has been written and approved by senior management. Employees should be instructed on how to comply with the security policies and the consequences of violation. The training program should point what a security threat looks like and the steps that employees can take to mitigate risks. It should also include a short description of the security controls and devices that are in place on the network.

## **Security Solution System Description**

The following presents a “defense-in-depth” network architecture for Netco that addresses the problems noted in the Risk Assessment and follows the guidelines and standards laid out by the security policy. A defense in depth strategy insures that every layer of the network is protected. The outside “edge” of the network that connects Netco to the internet and third party networks is hardened from intrusion but this is not a total solution. The internal systems of the network have also been designed with security from the ground up.

## Netco WAN



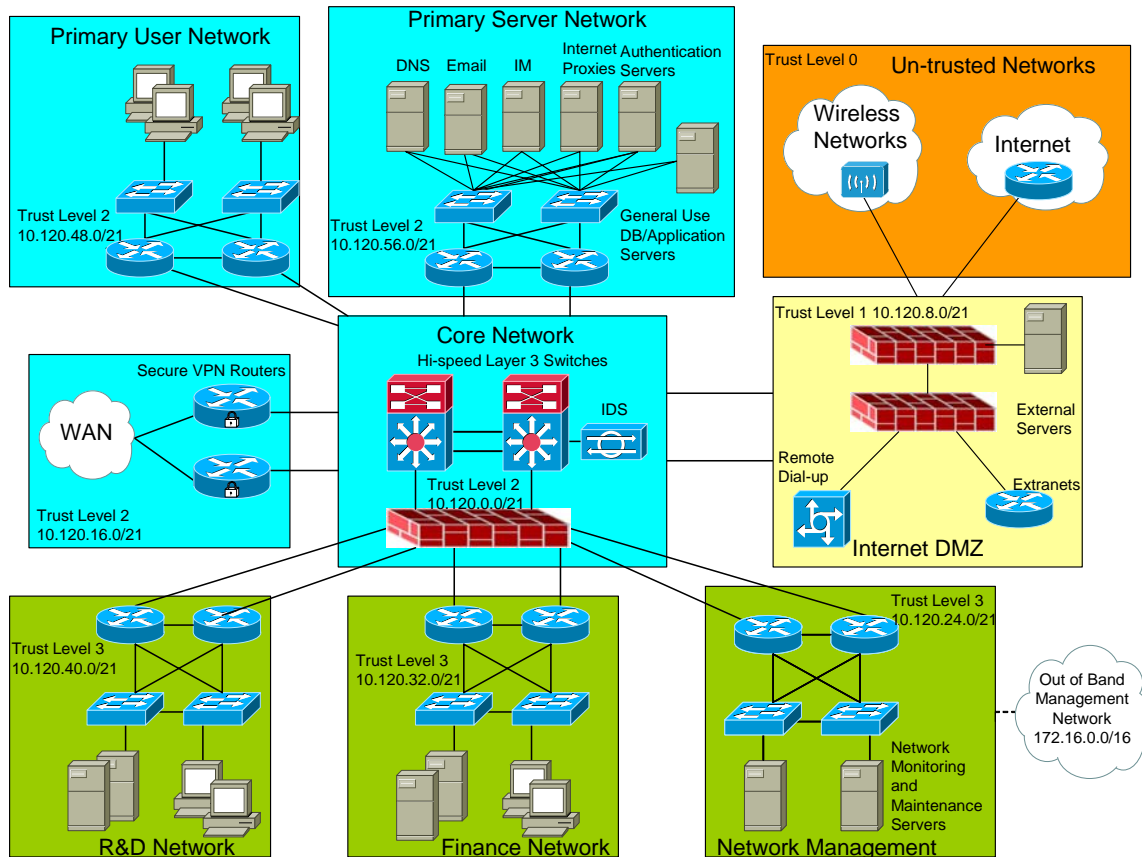
This diagram depicts the Netco Wide Area Network. The Dallas HQ contains the majority of the services that Netco employees use. The Brussels and Shanghai offices connect to Dallas using a private WAN, while the remote sales offices, teleworkers, and the fabrication facility connect through the internet. All of these connections are secured with an IP Sec Virtual Private Network. An IP SEC VPN uses cryptography to insure that the data being transferred stays confidential, is from an authorized source, and has not been tampered with during transit. The Shanghai and Brussels offices have permanent VPNs to the Dallas HQ over the private WAN. While there is much less risk of data interception over a private WAN, confidential data such as Netco designs will be transferred over the WAN. In keeping with the outlined security policies this data must be encrypted. This ensures that if the Netco network was

somehow penetrated, the most confidential data would still remain protected. The sales offices do not need the dedicated bandwidth of a private connection and the IPSEC VPN ensures that the communications between the sales offices and Netco remains secure even over a public network.

Remote Tele-workers and Sales People can utilize any internet connection to establish a secure link back to the Dallas HQ. A VPN client and a One Time Password Token are utilized to create a temporary VPN from remote workstation, through the internet to Netco HQ. This allows employees to work from home or wherever they may be.

In this design only the Dallas HQ has a connection to the internet from inside the Netco core network. Securing an internet connection is costly and requires constant maintenance and monitoring by the IT staff. Netco must weight the benefits of each office having their own internet connection versus the cost of securing each of those connections.

## Dallas HQ Network



This diagram illustrates the network of the Dallas HQ office. This Network is the largest as it contains the edge network which connects to the internet. The Network has been divided into 4 separate Trust domains each with a corresponding trust level. A trust level of 0 is a completely un-trusted network while a Trust level of 3 is the most trusted network domain.

**Trust Level 0:** The Internet, and all wireless networks

**Trust level 1:** The Internet DMZ network that separates the internal network from the internet, Third Party Extranets like the Fab Facility, and remote dialup access facilities.

**Trust Level 2:** The private Wide Area Network to the Shanghai and Brussels Offices and the General Use networks used by Netco Employees

**Trust Level 3:** The most sensitive parts of the network including the R&D and Finance departments, as well as the Management Network used by the IT and Security staff to maintain the network.

### **IP Address Plan**

The Netco network must have a well designed IP Plan. RFC 1918 defines Private IP Addressing. Private Addresses are IP addresses that are not used on the Internet. The largest IP space defined by RC 1918 is the 10.0.0.0/8 network. A portion of this network is used to define the internal IP space for Necto. Since RFC 1918 private addressing is used to define all internal addresses, all public addresses can be filtered out by the edge devices. Only the Devices on the edge of the network in the Internet DMZ should see public IP addresses. Additionally, All RFC 1918 addresses not in use by Netco can be filtered out. The IP Network used for the Dallas HQ is the 10.120.0.0/16 network. Each network domain is configured with a subnet of this network. Devices in the domains should only be given addresses in these ranges. This allows the routers and firewalls to easily control access between domains using Firewall Rules and Router access lists. The subnets have been laid out as follows:

- **Core Network:** 10.120.0.0/21
- **Internet DMZ:** 10.120.8.0/21
- **Internal WAN:** 10.120.16.0/21
- **Network Management:** 10.120.24.0/21
- **Finance Network:** 10.120.32.0/21
- **R&D Network:** 10.120.40.0/21
- **Primary User Network:** 10.120.48.0/21

- **General Server Network:** 10.120.56.0/21

This gives each domain 8 Class C networks with which to assign addresses. These networks can be further divided if needed. Additionally, the 172.16.0.0/16 private address space is used to define a separate logical network for Out of Band Management. An out of Band Management Network is the most secure method for managing and administrating network devices.

The Brussels and Shanghai Office utilize a similar plan using an overall network of 10.121.0.0/16 and 10.122.0.0/16 respectively. While these IP spaces may seem large, it is better for Netco to grow into a large IP space than have to redefine the networks as Netco increases in size.

### **HQ Network Domains**

All domains are connected through the *Core Network Domain*. A pair of redundant high speed layer 3 switches is used to quickly move traffic between the domains. No filtering of traffic occurs on the core switches, the purpose of this domain is to switch traffic between the domains in the most efficient manner possible. Filtering of Traffic occurs at the connection points between the Core network and the individual zones. The Server Network, User Network, and WAN, all utilize routers with access lists to filter traffic sent to the core. The Level 3 trust domain networks are protected with a firewall. The Internet DMZ separates the core from the un-trusted networks. The security features of the Internet DMZ are explained in a later section. Since all traffic passes through the core network, it is the perfect place to locate our Main IDS sensor. Any intrusion traffic must pass through the core and the sensor would detect it.

The *Primary User Network* contains most of the users of the network. R&D and Finance users are separated into their own domains. The users of this network are allowed to connect to the servers in the *Primary Server Network* in order to access email, databases, and the proxy servers for internet access. Access to the *Primary Server Networks* in the remote offices can also be granted if needed. The users in this domain will also be able to connect to the *Network Management Domain* in a limited way. The PCs will run a login script that verifies that their current level of patching and virus signatures. If an update is needed, the PC will contact the update servers in the Network Management Domain and acquire the updates before they are allowed access to the network. Redundant pairs of routers and switches are used to connect into the core network in order to protect the users from a network hardware failure.

The *R&D and Financial Domains* contain *most sensitive* data. The database and file servers used by each of these groups reside in their respective domains rather than the *Primary Server Network*. Access to these servers is restricted to users in their domain and outside access is only allowed from the *Network Management Domain*. If information or files need to be shared outside this domain, they can be placed in an encrypted directory on a file server in the *Primary Server domain*. Data can also be shared through email using a secure email client that ensures that the data can only be decrypted and read by someone who has the proper authority. To protect the sensitive data of these networks from loss each employs a separate backup system from the rest of the network. Encryption of these backups would further secure the data from loss. In all other respects, these domains function as the *General User Network*.

The *Wide Area Network* domain provides access to the Shanghai and Brussels offices over a private WAN. Redundant Secure VPN routers are used to encrypt any traffic that is sent to the other sites. Even though the WAN network is private, it resides outside the control of Netco. Encryption ensure that any data sent over the WAN links remains private and no one but the intended recipient (in this case the other WAN routers) can receive it.

The *Primary Server Network* provides network services and applications to all Netco Employees. All user domains are allowed to connect to the servers in this network. The following systems reside within the *Primary Server Network*:

*Email:* Inbound Email is scanned by an email antivirus and spam filtering server and then delivered to two redundant email servers. Users contact these servers to read or download their email. A separate server is used for outbound email. This server is allowed to connect to the SMTP mail servers in the *Internet DMZ* to deliver mail to the internet.

*DNS:* The primary and secondary internal Directory Name Servers provide name resolution for all internal devices. Requests for external DNS addresses are sent to a separate DNS forwarding server that is allowed to contact the external DNS servers located in the Internet DMZ.

*HTTP Proxy:* Internal Users are not allowed to access the Internet directly. A proxy-cache server is employed to provide access to internet websites. This server also caches commonly accessed pages to reduce the traffic load on the internet DMZ. In Addition, the server employs a content filter to block access to any websites that Netco deems inappropriate.

*Instant Messaging:* An internal Instant Messaging server allows Netco employees to communicate with each other using IM client. These clients can only chat with users on the Netco Network. It is not possible to chat with other people on the internet. IM is too great a security risk to allow this.

*General Use Servers:* Database and File Servers for general use are located in this domain. All access is controlled through the use of the *Identity Management and Authentication Servers*.

*Identity Management/Authentication:* Identity Management and Authentication can often be complicated. Network Logins, Applications Servers, and Remote Access all require different kinds of authentication. A Single Sign On (SSO) system allows the same password to be used for all internal access. This is utilized in combination with a root user Directory Server and AAA (Authentication, Authorization, and Accounting) servers to provide identity management and access control. Network logins and Application passwords are verified directly through the root user server. Access to network devices such as routers, switches, and firewalls is handled by a separate AAA located in the *Network Management Domain*.

*Remote Access* is handled through the use of a OTP (one time password) system. Remote access users must have a token that generates a one time password to gain access. The AAA servers provide access control for all remote access such as VPN and dial-up. The AAA servers contact the root user Server and the OTP system to verify usernames and passwords.

*Backup System:* A full network backup system ensures full backups of all servers on a regular basis.

The *Network Management* Domain is used by IT and security staff to administrate and monitor the network. This domain has access to the entire network including the Internet DMZ through the *Out of Band Management Network*. This is a secondary network that connects to all network and security devices that can only be accessed from inside the Network Management Domain. Access into this domain is limited to the Remediation servers that all users contact in order to update their computers. This Domain provides the following services:

*Remediation:* An automated patching system keeps the patch levels on all systems and servers in the network up to date. Virus and IDS update servers pull down the latest signatures and update the IDS sensors and Virus Scanning tools in the network. These systems also verify that workstations have been properly updated before allowing them to connect to the network.

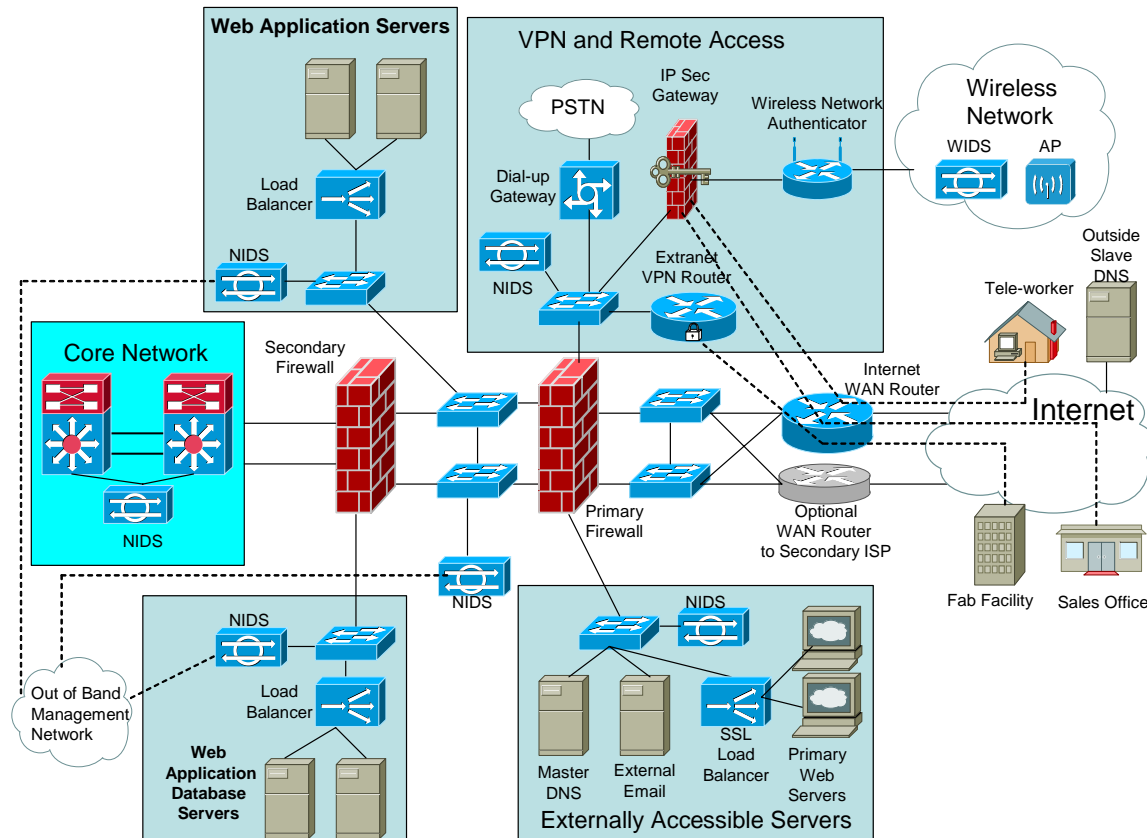
*Log Management:* A server collects log files from all network security devices and scans for unusual entries that may indicate an intrusion. The logs are correlated with data from the IDS sensors and network management system to present a full picture of network operation.

*Network Management and Monitoring:* All network devices report fault and diagnostic information through SNMP. Some applications can reports using SNMP information as well. An SNMP Manager is utilized to monitor this information and to gather performance data about the network. This allows for proactive monitoring of network problems as well as root cause analysis of problems when they occur. SNMP itself can be a security problem in order to mitigate this risk SNMP Version 3 will be used and utilize non-standard SNMP community strings.

*Identity Management:* The security devices and network equipment are the most vital parts of the network. Login access and Passwords must be tightly controlled. A separate Identity Management system is used to verify all logins and passwords for the security and network devices.

*Vulnerability Scanning:* Routine Vulnerability Scans of Netco's network ensures that any weaknesses in network security are quickly found. Any problems found by the vulnerability scanner are then corrected using the remediation tools.

### Internet DMZ



The *Internet DMZ* network defines the “edge” of Netco’s network. It serves as a buffer between the Netco network and external networks so that access can be controlled and managed. This network allows internal Netco users to connect to the

internet and remote networks in a secure fashion. It also provides secure remote access to the Netco network whether from a third party network, the internet, wireless networks, or dial-up facilities.

The *Internet DMZ* uses a pair of redundant stateful firewalls to separate the internal network from external access. In order to simplify the diagram only one firewall in each pair is shown. These firewalls define 4 separate sub-domains of trust within the internet DMZ. As these networks are the most vulnerable to attack, each sub-domain network has a Network Intrusion Detection sensor. These sensors are managed through the *Out of Band Management network* that connects to the *Network Management Domain*.

The *Core Network* connects to the secondary pair of redundant firewalls. The only traffic allowed on the core network is traffic that has passed through all the security features of the *Internet DMZ*. Strict rules are configured on the firewalls to define exactly what traffic is allowed through to the Core Network. A NIDs sensor is present on the core network to monitor for any abnormal traffic passing through the firewalls.

The *Web Application Database Servers* provide database services for any Web based applications such as E-commerce. These reside in a separate network from the application servers themselves so that access to them can be controlled by the secondary Firewall. Only the *Web Application Servers* are allowed to access these servers and perform database queries. A network load balancer is employed to ensure that traffic scales properly and is evenly distributed across the servers.

The *Web Application Servers* house any applications that are run from the Netco internet web servers. This network connects to a pair redundant network switches

located in between the two firewalls. The only connections allowed into this network are from the Netco web servers. The firewalls limit those connections to strictly what is necessary for the applications to function. A load balancer is employed here as well to manage network traffic.

The *Externally Accessible Servers* are servers that require access directly from the internet. This includes the Netco Web servers, the Master Internet DNS server, and the External Email Servers. This network is connected to a leg of the primary firewall pair. Access into this network is limited to the services that each server provides. An SSL load balancer is employed for the web servers in order to manage traffic and secure any E-commerce transactions. The secondary DNS server is located at an off site hosting company to provide redundancy for the Master DNS server.

The *VPN and Remote Access* network handles all remote connections into the Netco network. *Tele-workers and Sales offices* connect through the use of a software VPN. The connection terminates on the IP Sec gateway where the user is authenticated before allowing access to the internal network. The IP Sec gateway and the VPN client software form an encrypted tunnel between the Netco network and the remote users to ensure all data transferred remains private.

*Extranet Connections* such as the Fab facility utilize a similar IP SEC tunnel. Instead of using a software client, a permanent hardware VPN is employed. Access from the extranet network to the internal network is strictly controlled and limited to the servers that the third party need to access.

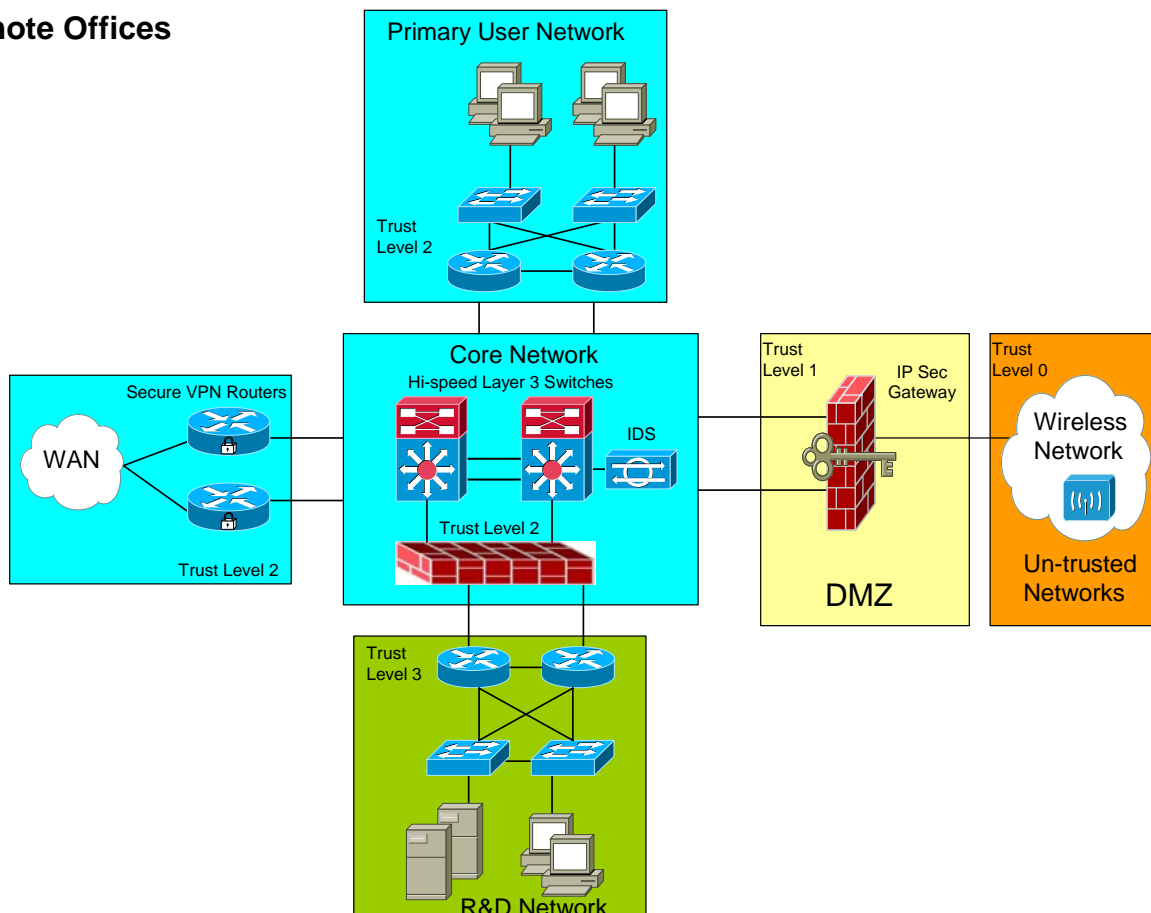
*Wireless Network Users* are treated in the same way as a remote Tele-worker. In order to get access to the wireless network they must first be authenticated by the

Identity Management system. The wireless network authenticator employs Wi-Fi protected access in order to secure this transaction. Once authenticated the user must establish an IP SEC VPN tunnel in order to access the internal network. A Wireless IDS is employed to scan for any rouge wireless APs or suspicious activity such as War Driving.

*Dial-up Users* connect in through a remote access gateway. This gateway utilizes the Identity Management system in the core network to validate any access.

The *Internet WAN Router* connects Netco to their Primary ISP. This router filters out any obviously bad address coming from the internet. All RFC 1918 and any non-routable address are filtered out. In addition it employs RFC 2827 Anti-spoof filtering to weed out possible spoofing attacks. If Netco requires a redundant connection to the internet a second WAN router can be employed and connected to a second ISP. This will provide continuous internet access should one ISP link or router fail.

## Remote Offices



The Shanghai and Brussels office networks are similar to the Dallas HQ office. The offices do not connect directly to the internet so an Internet DMZ is not needed. A mini-DMZ has been created to allow secure access from wireless networks. All network services are provided by the *General Use Servers* in the Dallas HQ and accessed through the Netco WAN. The R&D networks at the remote offices are protected in the same manner as the R&D networks in the Dallas HQ.

## **Summary**

There are many risks present on the Netco Network as it exists today. Netco is taking the right step by improving their network security. Netco's design data has almost certainly been exposed to unknown third parties and this has contributed to a loss of market share for Netco. This design presents a "defense-in-depth" security strategy that addresses Netco's business goals and ensures secure network operations.

Implementing secure network architecture can be costly and time consuming. The execution of this project will follow a phased approach, addressing the most critical risks first. In this way interruption to normal business operations is minimized and the cost is distributed over the course of the project.