Microsoft Business Solutions

Navision Security Hardening Guide

Published: October 2004

Microsoft

Contents

Introduction

Microsoft® Windows® provides sophisticated standards-based network security. In the broadest sense, security involves planning and considering tradeoffs. For example, a computer can be locked in a vault and only made accessible to one system administrator. This computer may be secure, but it is not very useful because it is not connected to any other computer. You need to consider how to make the network as secure as possible without sacrificing usability.

Most organizations plan for external attacks and construct firewalls, but many companies do not consider how to mitigate a security breach once a malicious user gets inside the firewall. Security measures in your client's environment will work well if users are not required to perform too many procedures and steps to conduct business in a secure manner. Implementing security policies should be as easy as possible for users or they will tend to find less secure ways of doing things.

Since the size of Navision installations can vary a great deal, it is important to carefully consider the needs of each client and weigh the effectiveness of security against the costs that may be involved. As your client's trusted advisor, use your best judgment and recommend a policy that meets their security needs without creating a burden that will ultimately cause the client to stop enforcing the policy.

Navision Security Best Practices

The following general rules can help increase the security of the Navision environment:

- If you want to run Navision Database Server as a service or use the *installasservice* command line parameter when you start the server, you should ensure that the service is running as the NT Authority\Network Service account. The NT Authority\Network Service account only exists on Windows™ XP and Windows Server™ 2003. If you are running Windows 2000 Server, you should create an account with least privileges for the service or else the service will be assigned a Local System account. This account should at the most have the same privileges as the normal Users account or be domain account that is not an administrator either in the domain or on any local computer.

  You must remember to give the NT Authority\Network Service account or the user account that the server is running under read and write access to the database file(s) to ensure that the users can connect to the database.

  To give the NT Authority\Network Service account read and write access to a database file on Windows XP:

  1. In Windows Explorer, navigate to the folder that contains the database file.
  2. Select the database file and right-click it and click Properties.
  3. In the ***Properties*** window, click the ***Security*** tab and under **Group and user names** field, click Add.
  4. In the ***Select Users, Computers, or Groups*** window, enter *Network Service* and click OK.
  5. NETWORK SERVICE has been added to the **Group and user names** field in the ***Properties*** window.
  6. Select NETWORK SERVICE and in the **Permissions** field give it *Read* and *Write* permission.

- The Navision Application Server service runs as the NT Authority\Network Service account by default and this allows it to access Navision Database Server locally. However, on a network you must ensure that the Navision Application Server service is running as a Windows domain account that is recognized by the Navision Database Server if you want it to have access to the database server. This account should not be an administrator either in the domain or on any local computer.

- If you are running the SQL Server Option for Navision, Microsoft SQL Server™ is running as a service. The SQL Server Option for Navision requires that SQL Server is able to look up Active Directory to get lists of Windows user groups for authentication purposes. You must therefore ensure that the SQL Server service is running as the NT Authority\Network Service account.

  To ensure that the service is running as NT Authority\Network Service:

  1. On the SQL Server computer locate the MSSQLSERVER service, right-click it and click Properties.
  2. In the ***Properties*** window, click the ***Log On*** tab.
  3. In the ***Log On*** tab, under Log on as click This Account and enter *NT Authority\NetworkService* and click OK.

  For more information about SQL Server security visit:

  http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx

  and http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx

- If you are running a Navision E-business product like Commerce Gateway, you should ensure that the Commerce Gateway Request Server has been installed correctly with the default account setting for the services. The default account setting is called *CGRSUser* and grants Commerce Gateway Server access to the minimum set of other services that it requires, including the *MSSQLSERVER* service and *BizTalk Service BizTalk Group : BizTalkServerApplication* and does not include any global account settings like the *Local System* account does.
- Always use strong passwords. For more information about strong passwords, see the section Strong Passwords.
- Use Windows Logins. Navision allows you to create two kinds of logins – Database Logins and Windows Logins. We recommend that you use Windows Logins because this uses Windows Authentication and allows you enforce a proper password policy.
- Passwords should not be reused. It is often common practice to reuse passwords across systems and domains. For example, an administrator responsible for two domains might create Domain Administrator accounts in each that use the same password, and even set local administrator passwords on domain computers that are the same across the domain. In this case, if a single account or computer is compromised this can lead to the entire domain being compromised.
- After Navision is installed and the databases are created, or updated, you should create a Windows Login and assign it the SUPER role in Navision. This SUPER user will manage database administration, security and so on. Give this login a strong password. This password should be kept confidential. It should warrant the same protection you give to the SA password in SQL Server. All database access is managed by the SUPER role and it requires the highest level of protection. The SUPER user's password should only be known to your System Administrators.
- All the other users who have access to the Navision database should run with least privilege. This means assigning them roles in Navision that only give them access to the features and functionality that they need to perform their tasks in the company.
- Ensure that only those users whose role within the company requires it are able to import FOB files, redesign objects as well as create and restore database backups.
- Make regular backups of your Navision database and remember to test the backups to ensure that they can be restored successfully.
- Store your backups in a safe place to limit the impact from hazards like fire, smoke, dust, high temperature, lightning, and environmental disasters (for example, an earthquake).
- Although Navision can run on several versions of Windows, we recommend that you use the newest operating systems with the most up-to-date security features. This is currently Windows XP, Service Pack 2 and Windows Server 2003.
- Use the Windows Update service provided with Windows 2000, Windows XP, and Windows Server 2003 to apply the most recent security updates. Use the Automatic Update feature of Windows to keep all your client computers up to date with the most recent security patches, service packs and updates.
- We recommend that you use the TCPS secure protocol to communicate between the Navision clients and Navision Database Server. TCPS is a secure version of TCP/IP and uses the Security Support Provider Interface (SSPI) with encryption enabled and Kerberos authentication. TCPS is the default protocol for Navision Database Server.
- The customer should have a disaster recovery plan that ensures the rapid resumption of services after a disaster. A recovery plan should include issues like:
    - Acquiring new/temporary equipment.
    - Restoring backups onto new systems.
    - Testing that the recovery plan actually works.

Physical Security

Physical security is absolutely imperative as there is no way to supplement it with software security. For example, if a hard disk drive is stolen, eventually the data on that drive will be stolen as well. Discuss the following physical security issues when developing a policy with your client:

- For large installations with dedicated IT departments, ensure that server rooms and places where software is stored are locked.
- Machines in this category include:
  - The Microsoft SQL Server 2000 server
  - The File Server where the Navision executables reside.
- Keep unauthorized users away from the computers.
- Ensure burglar alarms are installed, regardless of how sensitive the data is.
- Ensure backups of critical data are stored offsite and that backups are stored in fireproof containers.

The Employees

It is a good idea to limit administrative rights across all products and features. As a default, clients should give their employees only read access to system functions, unless they require greater access to perform their jobs. Microsoft suggests following the principle of least privilege: give users only the minimum privileges required to access data and functionality.
Disgruntled and former employees are a threat to network security. When discussing security with your clients, suggest the following policy regarding employees:

- Conduct pre-employment background investigations.
- Expect "revenge" from disgruntled employees and former employees.
- Make sure that they disable all the associated Windows accounts and passwords when an employee leaves. For reporting purposes, do not delete users. Do not reuse the accounts.
- Train users to be alert and to report suspicious activity.
- Do not grant privileges automatically. If users do not need access to particular computers, computer rooms, or sets of files, ensure that they do not have access.
- Train supervisors to identify and respond to potential employee problems.
- Make sure that employees understand their roles in maintaining network security.
- Give a copy of the company policies to every employee.
- Do not allow users to install software that is not authorized by their employers.

The Administrator

We recommend that your clients' system administrators keep up with the latest security fixes available from Microsoft. Attackers are very adept at combining small bugs to enable large intrusions into a network. Administrators should first ensure that each individual computer is as secure as possible, and then add security updates and use anti-virus software. Many links and resources are provided throughout this guide to help you find valuable information and best practices.

Complexity comprises another tradeoff for securing your network. The more complex the network, the more difficult it is to secure or fix once an intruder has successfully gained access. The administrator should document the network topography thoroughly, with the aim of keeping it as simple as possible.

Security is primarily concerned with risk management. Because technology is not a cure-all, security requires a combination of technology and policy. In other words, there will never be a product that you can simply unpack and install on the network that instantly achieves perfect security. Security is a result of both technology and policy — that is, it is how the technology is used that ultimately determines the security level of a network. Microsoft delivers security-conscious technology and features, but only the administrator, with your guidance, can determine the right policies for each organization. Be sure to plan for security early in the implementation and deployment process. Understand what your client wants to protect and what they are willing to do to protect it.

Finally, develop contingency plans for emergencies before they happen. Combine thorough planning with solid technology and your client will have great security.

For more information about security in general, see "The Ten Immutable Laws of Security Administration," at:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx.

and the articles on security management at:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Securing the Server Operating System

Although you may find many smaller customers do not have a server operating system, it is important that you understand and can communicate security best practices to larger customers with more complex network environments. You should also be aware that many of the policies and practices described in this document can easily be applied to those customers that only have client operating systems.

The concepts in this section apply to both the Microsoft Windows 2000 Server and Microsoft Windows Server 2003 products, although this information has been extracted mainly from Windows Server 2003 Online Help. Windows Server 2003 offers a robust set of security features. Windows Server 2003 Online Help contains complete information about all the security features and procedures.

For additional information about Windows 2000 Server, visit the Windows 2000 Server Security Center, at
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx.

and read the Windows 2000 Security Hardening Guide at:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

For additional information about Windows Server 2003, see the *Windows Server 2003 Security Guide*, at http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

The primary features of the Windows server security model are authentication, access control, and single sign-on:

- Authentication is the process by which the system validates a user's identity through their logon credentials. A user's name and password are compared against an authorized list. If the system detects a match, authorization grants the user access to the extent specified in the permissions list for that user.
- Access control limits user access to information or computing resources based on the users' identity and their membership of various predefined groups. Access control is typically used by system administrators for controlling the access that users have to network resources such as servers, directories, and files. This is typically implemented by granting users and groups permission to access specific objects.
- Single sign-on allows a user to log on to the Windows domain once, using a single password, and authenticate to any computer in the Windows domain. Single sign-on enables administrators to implement password authentication across the Windows network, while providing end users with ease of access.

The following sections contain more detailed descriptions of these three key features.

Authentication

Authentication is a fundamental aspect of system security and is used to confirm the identity of any user trying to log on to a domain or access network resources. The weak link in most authentication systems is the user's password.

Passwords provide the first line of defense against unauthorized access to the domain and local computers. Recommend the following password best practices:

- Always use strong passwords.
- If passwords must be written down on a piece of paper, store the paper in a secure place and destroy it when it is no longer needed.
- Never share passwords with anyone.
- Use different passwords for all user accounts.
- Change passwords at regular intervals.
- Be careful about where passwords are saved on computers.

Strong Passwords

The role that passwords play in securing an organization's network is often underestimated and overlooked. As mentioned earlier, passwords provide the first line of defense against unauthorized access to your network. You should therefore ensure that your clients instruct their employees to use strong passwords.

However, password-cracking tools continue to improve, and the computers used to crack passwords are more powerful than ever. Given enough time, the automated password-cracking tool can crack any password. Nevertheless, strong passwords are much harder to crack than weak passwords.

For guidelines in creating strong passwords that the user can remember, see

http://www.microsoft.com/athome/security/privacy/password.mspx

and

http://www.microsoft.com/ntworkstation/technicalresources/PWDguidelines.asp

Defining the Password Policy

When helping your client to define their password policy, be sure to create a policy that requires all the user accounts to have strong passwords. For most systems, following the recommendations in the Windows Server 2003 Security Guide are sufficient:

- Define the **Enforce password history** policy setting so that several previous passwords are remembered. With this policy setting, users cannot use the same password when their password expires.

  Recommended setting: 24

- Define the **Maximum password age** policy setting so that passwords expire as often as necessary for the client's environment.

  Recommended setting: between 42 (the default) and 90.

- Define the **Minimum password age** policy setting so that passwords cannot be changed until they are more than a certain number of days old. This policy setting works in combination with the **Enforce password history** policy setting. If a minimum password age is defined, users cannot repeatedly change their passwords to get around the **Enforce password history** policy setting and then use their original passwords. Users must wait the specified number of days to change their passwords.

  Recommended setting: 2.

- Define a **Minimum password length** policy setting so that passwords must consist of at least a specified number of characters. Long passwords, seven or more characters, are usually stronger than short ones. With this policy setting, users cannot use blank passwords and they must create passwords that are at least a certain number of characters long.

  Recommended setting: 8.

- Enable the **Password must meet complexity requirements** policy setting. This policy setting checks all new passwords to ensure that they meet basic strong password requirements. This setting ensures that passwords have at least three symbols from the four categories (upper-case, lower-case, numbers, non-alphanumeric symbols), and that it does not contain any portion of the user name and the first or last name of the user.

  Note
  Passwords that meet these requirements are not necessarily very strong. For instance, the password “Password1” meets these requirements.

  Recommended setting: Yes

- For a full list of these requirements, see "Password Must Meet Complexity Requirements" in Windows Server Online Help.
- Store passwords using reversible encryption – Reversible encryption is used in systems where an application needs access to clear-text passwords. It is not needed in most deployments.

  Recommended setting: No.

For more information, see the Windows Server 2003 Security Guide:

http://www.microsoft.com/technet/security/prodtech/Win2003/W2003HG/SGCH00.mspx

Defining an Account Lockout Policy

Be cautious when defining the account lockout policy. The account lockout policy should never be set in a small business as it is also highly likely to lock out authorized users and this can be very costly for your client.

If the client decides to apply account lockout policy, set the **Account lockout threshold policy** setting to a high enough number that authorized users are not locked out of their user accounts simply because they mistype their password several times.

For more information about account lockout policy, see "Account Lockout Policy Overview" in Windows Server Online Help.

For information about how to apply or modify account lockout policy, see "To Apply or Modify Account Lockout Policy" in Windows Server Online Help.

Access Control

A Windows network and its resources (including Navision) can be secured by considering what rights users, groups of users, and other computers have on the network. You can secure a computer or multiple computers by granting users or groups specific user rights. You can secure an object, such as a file or folder, by assigning permissions that allow users or groups to perform specific actions on that object. Key concepts that make up access control include:

- Permissions
- Ownership of objects
- Inheritance of permissions
- User rights
- Object auditing

Permissions

Permissions define the type of access granted to a user or group for an object or object property such as files, folders, and registry objects. Permissions are applied to any secured objects such as files or registry objects. Permissions can be granted to any user, group, or computer. It is a good practice to assign permissions to groups.

Ownership of Objects

An owner is assigned to an object when that object is created. By default in Windows 2000 Server, the owner is the creator of the object. This has changed in Windows Server 2003 for objects created by members of the Administrators group.

When a member of the Administrators group creates an object in Windows Server 2003, the Administrators group becomes the owner, rather than the individual account that created the object. This behavior can be changed through the Local Security Settings Microsoft Management Console (MMC) snap-in, using the setting **System objects: Default owner for objects created by members of the Administrators group**. No matter what permissions are set on an object, the owner of the object can always change the permissions on an object.

For more information, see "Ownership" in Windows Server Online Help.

Inheritance of Permissions

Inheritance allows administrators to easily assign and manage permissions. This feature automatically causes objects within a container to inherit all the inheritable permissions of that container. For example, when you create files within a folder they inherit the permissions of the folder. Only the permissions marked to be inherited are inherited.

User Rights

User rights grant specific privileges and logon rights to users and groups in your computing environment.

For information about user rights, see "User Rights" in Windows Server Online Help.

Object Auditing

You can audit users' access to objects. You can then view these security-related events in the security log using the Event Viewer.

For more information, see "Auditing" in Windows Server Online Help.

Access Control Best Practices

- Assign permissions to groups rather than to users. Because it is inefficient to maintain user accounts directly, assigning permissions on a user basis should be the exception.
- Use Deny permissions for certain special cases. For instance, you can use Deny permissions to exclude a subset of a group which has Allow permissions.

- Never deny the Everyone group access to an object. If you deny everyone permission to an object, that also includes the administrators. A better solution would be to remove the Everyone group, as long as you give other users, groups, or computers permissions to that object. Remember that if no permissions are defined then no access is allowed.
- Assign permissions to an object as high on the tree as possible and then apply inheritance to propagate the security settings throughout the tree. You can quickly and effectively apply access control settings to all children or a sub-tree of a parent object. By doing this, you gain the greatest breadth of effect with the least effort. The permission settings you establish should be adequate for the majority of users, groups, and computers.
- Explicit permissions can sometimes override inherited permissions. Inherited Deny permissions do not prevent access to an object if the object has an explicit Allow permission entry. Explicit permissions take precedence over inherited permissions, even inherited Deny permissions.
- For permissions on Active Directory® objects, make sure you understand the best practices specific to Active Directory objects.

For more information, see "Best Practices for Assigning Permissions on Active Directory Objects" in Windows Server 2003 Online Help.

External Security Firewall

A firewall is a piece of hardware or software that prevents data packets from either entering or leaving a specified network. To control the flow of traffic, ports in the firewall are either opened or closed to information packets. The firewall looks at several pieces of information in each data packet: the protocol through which the packet is being delivered, the destination or sender of the packet, the type of content that is contained in the packet, and the port number to which it is being sent. If the firewall is configured to accept the specified protocol through the targeted port, the packet is allowed through. Microsoft Windows Small Business Server 2003 Premium Edition ships with Microsoft Internet Security and Acceleration (ISA) Server 2000 as its firewall solution. Small Business Server Standard Edition also includes a firewall.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 securely routes requests and responses between the Internet and client computers on the internal network.

ISA Server acts as the secure gateway to the Internet for clients on the local network. The ISA Server computer is transparent to the other parties in the communication path. The Internet user should not be able to tell that a firewall server is present, unless the user attempts to access a service or go to a site where the ISA Server computer denies access. The Internet server that is being accessed interprets the requests from the ISA Server computer as if the requests originated from the client application.

When you choose Internet Protocol (IP) fragment filtering, you enable the Web Proxy and Firewall services to filter packet fragments. By filtering packet fragments, all fragmented IP packets are dropped. A well-known "attack" involves sending fragmented packets and then reassembling them in such a way that may cause harm to the system.

ISA Server features an intrusion detection mechanism, which identifies the time when an attack is attempted against a network and performs a set of configured actions (or alerts) in case of an attack.

If Internet Information Services (IIS) is installed on the ISA Server computer, you must configure it to not use the ports that ISA Server uses for outgoing Web requests (by default, 8080) and for incoming Web requests (by default, 80). For example, you can change IIS to monitor port 81, and then configure the ISA Server computer to direct the incoming Web requests to port 81 on the local computer running IIS.

If there is a conflict between ports that ISA Server and IIS use, the setup program stops the IIS publishing service. You can then change IIS to monitor a different port and restart the IIS publishing service.

ISA Server Policies

You can define an ISA Server policy that dictates inbound and outbound access. Site and content rules specify which sites and content can be accessed. Protocol rules indicate whether a particular protocol is accessible for inbound and outbound communication.

You can create site and content rules, protocol rules, Web publishing rules, and IP packet filters. These policies determine how the ISA Server clients communicate with the Internet and what communication is permitted.

Virus Protection

A computer virus is an executable file that is designed to replicate itself, erase or corrupt data files and programs, and avoid detection. In fact, viruses are often rewritten and adjusted so that they cannot be detected. Viruses are often sent as e-mail attachments. Antivirus programs must be updated continuously to look for new and modified viruses. Viruses are the number one method of computer vandalism.

Antivirus software is specifically designed for the detection and prevention of virus programs. Because new virus programs are created all the time, many makers of antivirus products offer periodic updates of their software to customers. Microsoft strongly recommends implementing antivirus software in your client's environment.

Virus software is usually installed at each of these three places: user workstations, servers, and the network where e-mail comes into (and in some cases, leaves) the organization.

Types of Viruses

There are three main types of viruses that infect computer systems: boot-sector viruses, file-infecting viruses, and Trojan horse programs.

Boot-Sector Viruses

When a computer starts, it scans the boot sector of the hard disk before loading the operating system or any other startup files. A boot-sector virus is designed to replace the information in the hard disk's boot sectors with its own code. When a computer is infected with a boot-sector virus, the virus' code is read into memory before anything else. After the virus is in memory, it can replicate itself onto any other disks that are in use in the infected computer.

File-Infecting Viruses

The most common type of virus, a file-infecting virus, attaches itself to an executable program file by adding its own code to the executable file. The virus code is usually added in such a way that it escapes detection. When the infected file is run, the virus can attach itself to other executable files. Files infected by this type of virus usually have a .com, .exe, or .sys file name extension.

Some file-infecting viruses are designed for specific programs. Program types that are often targeted are overlay (.ovl) files and dynamic-link library (.dll) files. Although these files are not run, executable files call them. The virus is transmitted when the call is made.

Damage to data occurs when the virus is triggered. A virus can be triggered when an infected file is run or when a particular environment setting is met (such as a specific system date).

Trojan Horse Programs

A Trojan horse program is not really a virus. The key distinction between a virus and a Trojan horse program is that a Trojan horse program does not replicate itself; it only destroys information on the hard disk. A Trojan horse program disguises itself as a legitimate program, such as a game or utility. When it's run, though, it can destroy or scramble data.

Virus Protection Best Practices

The spread of a macro virus can be prevented. Here are some tips to avoid infection that you should share with your clients:

- Install a virus protection solution that scans incoming messages from the Internet for viruses before the messages pass the router. This will ensure that e-mails are scanned for known viruses.
- Know the source of the documents that are received. Documents should not be opened unless they are from someone the client feels is trustworthy.

- Talk to the person who created the document. If the users are at all unsure whether the document is safe, they should contact the person who created the document.
- Use the Microsoft Office macro virus protection. In Office, the applications alert the user if a document contains macros. This feature allows the user to either enable or disable the macros as the document is opened.
- Use virus-scanning software to detect and remove macro viruses. Virus-scanning software can detect and often remove macro viruses from documents. Microsoft recommends the use of antivirus software that is certified by the International Computer Security Association (ICSA).

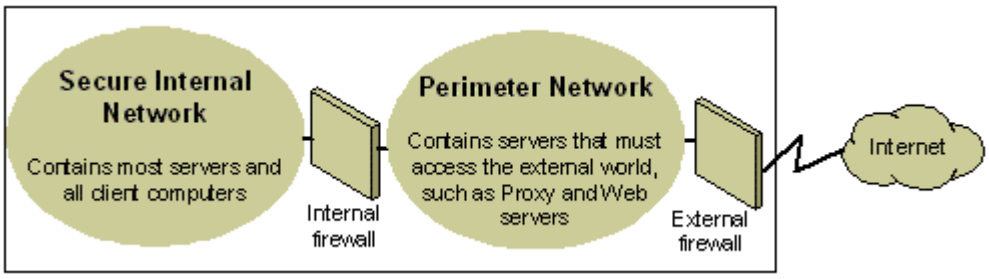
For more information about viruses and computer security in general, visit the following Microsoft Security websites:

- Microsoft Security at http://www.microsoft.com/security/default.asp.
- Security documentation on Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx.

Network Security Strategies

Because the design and deployment of an IP internetworking environment requires balancing private and public network concerns, the firewall has become a key ingredient in safeguarding network integrity. A firewall is not a single component. The National Computer Security Association (NCSA) defines a firewall as "a system or combination of systems that enforces a boundary between two or more networks." Although different terms are used, that boundary is frequently known as a perimeter network. The perimeter network protects your intranet or enterprise local area network (LAN) from intrusion by controlling access from the Internet or other large networks.

The following diagram shows a perimeter network bounded by firewalls and placed between a private network and the Internet in order to secure the private network:



Basic Perimeter Network

Organizations vary in their approach to using firewalls for providing security. IP packet filtering offers weak security, is cumbersome to manage, and is easily defeated. Application gateways are more secure than packet filters and easier to manage because they pertain only to a few specific applications, such as a particular e-mail system. Circuit gateways are most effective when the user of a network application is of greater concern than the data being passed by that application. The proxy server is a comprehensive security tool that includes an application gateway, safe access for anonymous users, and other services. Here is some information about these different options:

- **IP Packet Filtering**
  IP packet filtering was the earliest implementation of firewall technology. Packet headers are examined for source and destination addresses, Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) port numbers, and other information. Packet filtering is a limited technology that works best in clear security environments where, for example, everything outside the perimeter network is not trusted and everything inside is. In recent years, various vendors have improved on the packet filtering method by adding intelligent decision-making features to the packet-filtering core, thus creating a new form of packet filtering called *stateful protocol inspection*. You can configure packet filtering to either accept specific types of packets while denying all others or to deny specific types of packets and accept all others.
- **Application Gateways**
  Application gateways are used when the actual content of an application is of greatest concern. That they are application-specific is both their strength and their limitation, because they do not adapt easily to changes in technology.
- **Circuit Gateways**
  Circuit gateways are tunnels built through a firewall connecting specific processes or systems on one side with specific processes or systems on the other. Circuit gateways are best employed in situations where the person using an application is potentially a greater risk than the information carried by the application. The circuit gateway differs from a packet filter in its ability to connect to an out-of-band application scheme that can add additional information.
- **Proxy Servers**
  Proxy servers are comprehensive security tools, which include firewall and application gateway functionality that manage Internet traffic to and from a LAN. Proxy servers also provide document caching and access control. A proxy server can improve performance by caching and directly supplying frequently requested data, such as a popular Web page. A proxy server can also filter and discard requests that the owner does not consider appropriate, such as requests for unauthorized access to proprietary files.

Be sure the client takes advantage of those firewall security features that can help them. Position a perimeter network in the network topology at a point where all traffic from outside the corporate network must pass through the perimeter maintained by the external firewall. You can fine-tune access control for the firewall to meet the client's needs and can configure firewalls to report all attempts at unauthorized access.

To minimize the number of ports that you need to open on the inner firewall, you can use an application layer firewall, such as ISA Server 2000.

For more information about TCP/IP, see "Designing a TCP/IP Network" at http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Wireless Networks

By default, wireless networks are typically configured in a manner that allows eavesdropping on the wireless signals. They can be vulnerable to a malicious outsider gaining access because of the default settings on some wireless hardware, the accessibility that wireless networks offer, and present encryption methods. There are configuration options and tools that can protect against eavesdropping but keep in mind that they do nothing to protect the computers

from hackers and viruses that enter through the Internet connection. Therefore, it is extremely important to include a firewall to protect the computers from unwanted intruders on the Internet.

For more information about protecting a wireless network, see "How to Make Your 802.11b Wireless Home Network More Secure" at http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Network Security Scenarios

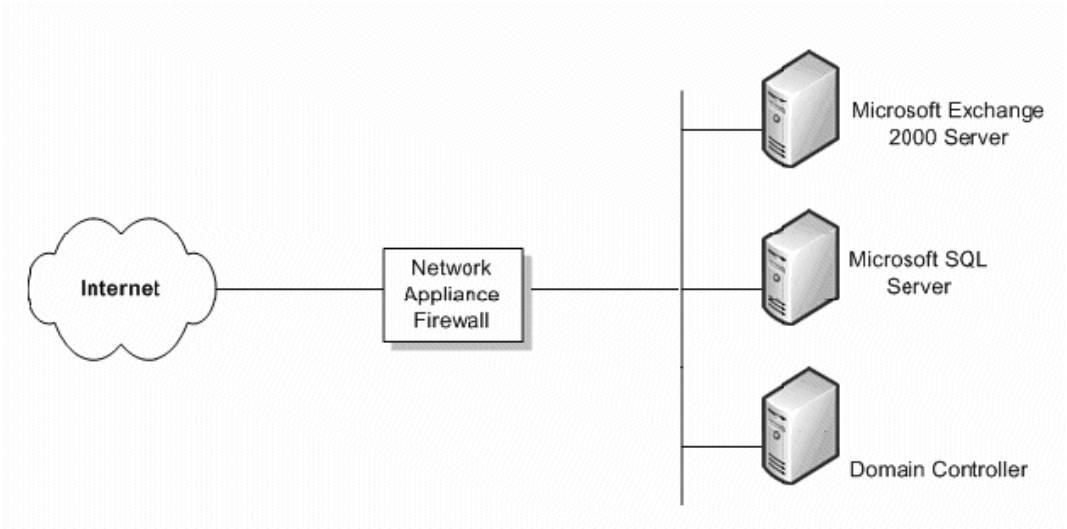
The level of network security that the client's organization requires depends on several factors. It usually comes down to a compromise between budget and the need to keep the corporate data safe. It is possible for a small business to have a very complex security structure that provides the highest possible level of network security, but a small business may not be able to afford that level of security. In this section, we look at four scenarios and make recommendations in each that provide varying levels of security.

No Firewall

If your client has a connection to the Internet but no firewall, some measure of network security needs to be implemented. There are simple network firewall appliances that provide enough security to deter most would-be hackers.

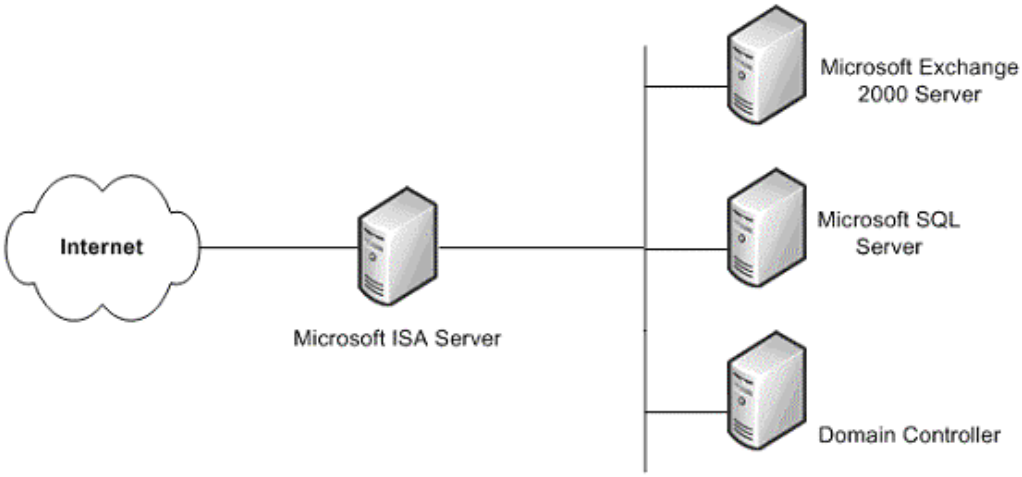
One Simple Firewall

The minimum level of security recommended is a single firewall between the Internet and your client's data. This firewall may not provide any level of advanced security and should not be considered very secure. But it is better than nothing.



Simple Firewall

Hopefully, the client's budget will allow for a more secure solution that will protect their corporate data. One such solution is ISA Server. The increased cost of this additional server provides a great deal more security than your average consumer firewall, since they typically only provide network address translation (NAT) and packet filtering.



ISA Server Firewall

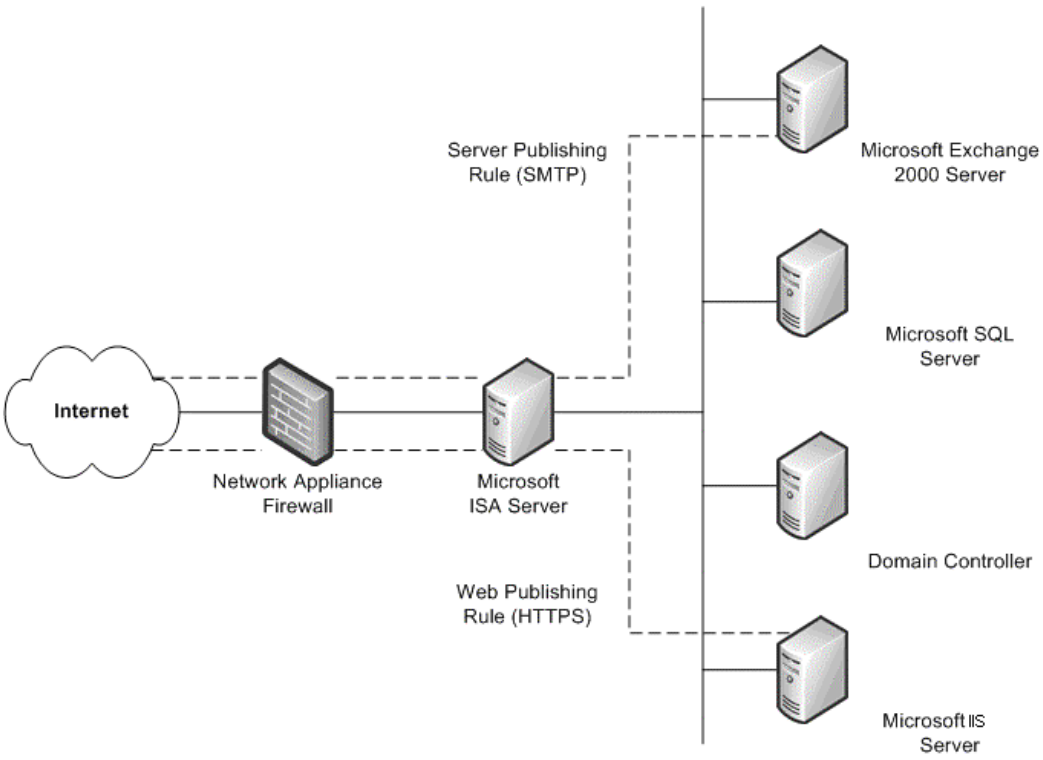
This single firewall solution is more secure than an entry level firewall appliance and provides Windows–specific security services.

One Existing Firewall

If the client has an existing firewall that separates their intranet from the Internet, you may want to consider an additional firewall that provides multiple ways to configure internal resources to the Internet.

One such method is Web publishing. This is when an ISA Server is deployed in front of an organization's Web server that is providing access to Internet users. With incoming Web requests, ISA Server can impersonate a Web server to the outside world, fulfilling client requests for Web content from its cache. ISA Server forwards requests to the Web server only when the requests cannot be served from its cache.

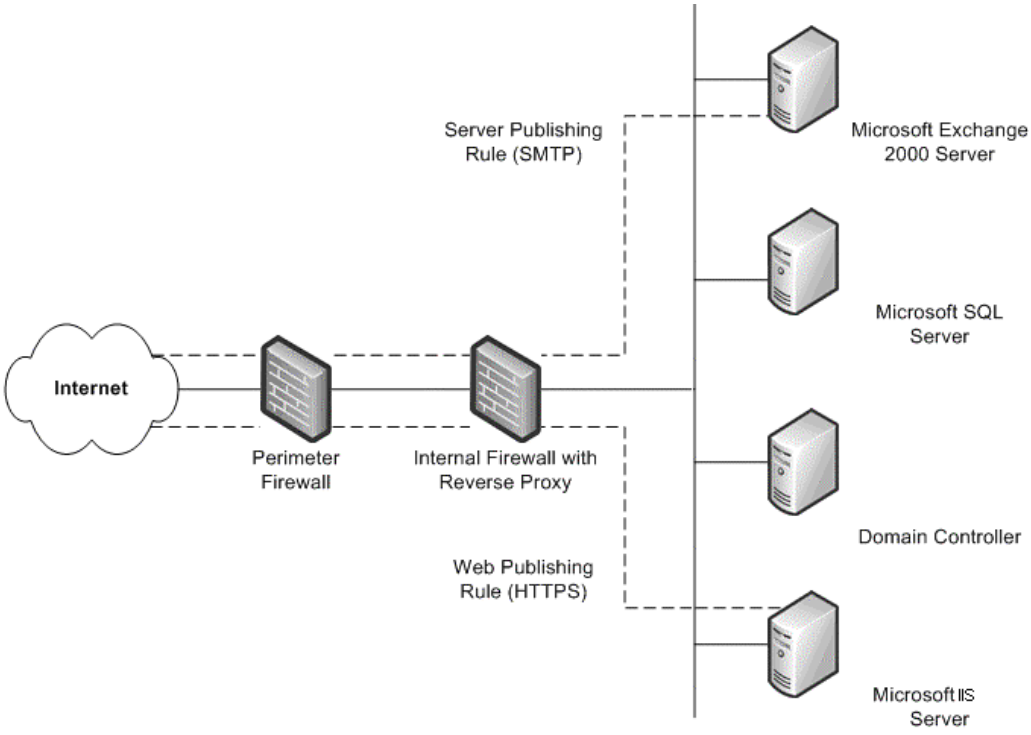
Another method is server publishing. ISA Server allows publishing internal servers to the Internet without compromising the security of the internal network. You can configure Web publishing and server publishing rules that determine which requests should be sent to a server on the local network, providing an increased layer of security for the internal servers.



Existing Firewall with ISA Server Added

Two Existing Firewalls

The fourth scenario is where the organization has two firewalls in place with an established perimeter network (DMZ). One or more of these servers is providing reverse proxy services so that Internet clients are not accessing servers on the intranet directly. Instead, one of the firewalls, ideally the internal firewall, is intercepting network requests for internal servers, inspecting those packets, and then forwarding them on behalf of the Internet host.



Two Existing Firewalls

This scenario is similar to the preceding scenario after the second firewall is added. The only difference is that the internal firewall that supports reverse proxy is not an ISA Server. In this scenario, you should work closely with the managers of each firewall to define server publishing rules that adhere to the security policy.

Security Patch Management

Operating systems and applications are often immensely complex. They can consist of millions of lines of code, written by many different programmers. It is essential that the software works reliably and does not compromise the security or stability of the IT environment. To minimize any problems, programs are tested thoroughly before release. However, attackers continually strive to find weaknesses in software, so anticipating all future attacks is not possible.

For many organizations, patch management form a part of their overall change and configuration management strategy. However, whatever the nature and size of the organization, it is vital to have a good patch management strategy, even if the organization does not yet have effective change and configuration management in place. The vast majority of successful attacks against computer systems occur to those systems where security patches have not been installed.

Security patches present a specific challenge to most organizations. Once a weakness has been exposed in software, attackers will generally spread information about it quickly throughout the hacker community. When a weakness occurs in its software, Microsoft strives to release a security patch as soon as possible. Until the patch is deployed, the security the client depends upon and expects may be severely diminished.

In the Navision environment, you must ensure that your clients have the most recent security patches installed throughout their system. Make sure the client uses one the technologies that Microsoft has made available. These include:

- **Microsoft Security Notification Service**
  The Security Notification Service is an e-mail list that distributes notices whenever an update becomes available. These notices serve as a valuable piece of a proactive security strategy. They are also available at the TechNet Product Security Notification website: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Microsoft Automatic Updates**
  Windows can automatically apply security updates to your machines.
- **Microsoft Security Bulletin Search Tool**
  The Security Bulletin search tool is available at the Security Bulletin Service website: http://www.microsoft.com/technet/security/current.aspx. The client can determine which updates they need based on the operating system, applications, and service packs they are currently running.
- **Microsoft Baseline Security Analyzer (MBSA)**
  This graphical tool is available at the Microsoft Baseline Security Analyzer website: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. This tool works by comparing the current status of a computer against a list of updates maintained by Microsoft. MBSA also performs some basic security checks for password strength and expiration settings, guest account policies, and a number of other areas. MBSA also will look for vulnerabilities in Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000, and Exchange Server 2003.
- **Microsoft Software Update Services (SUS)**
  Formerly known as Windows Update Corporate Edition, this tool enables enterprises to host on local computers all critical updates and security rollup packages (SRPs) available on the public Windows Update site. This tool works with a new release of automatic update (AU) clients to form the basis for a powerful automatic download and install strategy. The new AU client set includes a client for Windows 2000 and Windows Server 2003 operating systems and has the ability to automatically install downloaded updates. For more information about Microsoft SUS, see http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.
- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  The SMS Software Update Services Feature Pack contains a number of tools aimed at easing the process of issuing software updates throughout the enterprise. The tools include a Security Update Inventory Tool, a Microsoft Office Inventory Tool for Updates, the Distribute Software Updates Wizard, and an SMS Web Reporting Tool with Web Reports Add-in for Software Updates. For more information about each tool, see http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Talk to your clients about each of these tools and encourage their use. It is very important that security issues are addressed as quickly as possible, while maintaining the stability of the environment.

SQL Server 2000 Security Settings

As Navision also runs on SQL Server 2000, it is important that you take measures to increase the security of the client's SQL Server 2000 installation. The following steps will help increase SQL Server security:

- Make sure that the latest operating system and SQL Server 2000 service packs and updates are installed. For the latest details, check the Microsoft Security website http://www.microsoft.com/security/default.asp.
- For file system-level security, make sure all SQL Server 2000 data and system files are installed on NTFS partitions. You should make the files accessible only to administrative or system-level users through NTFS permissions. This will safeguard against users accessing those files when the MSSQLSERVER service is not running.
- Use a low-privilege domain account such as NT Authority\Network Service or the LocalSystem (recommended) account for SQL Server 2000 service (MSSQLSERVER). This account should have minimal rights in the domain and should help contain (but not stop) an attack to the server in case of compromise. In other words, this account should have only local user-level permissions in the domain. If SQL Server 2000 is using a Domain Administrator account to run the services, a compromise of the server will lead to a compromise of the entire domain. To change this setting, use SQL Server Enterprise Manager to make the change. The access control lists (ACLs) on files, the registry, and user rights will be changed automatically.
- Most editions of SQL Server 2000 are installed with two default databases, **Northwind** and **pubs**. Both databases are sample databases that are used for testing, training, and for general examples. They should not be deployed within a production system. Knowing that these databases are present can encourage an attacker to attempt exploits involving default settings and default configuration. If **Northwind** and **pubs** are present on the production SQL Server 2000 computer, they should be removed.
- Auditing of the SQL Server 2000 system is disabled by default, so no conditions are audited. This makes intrusion detection difficult and aids attackers in covering their tracks. At a minimum, you should enable auditing of failed logins.

For the most up-to-date SQL Server 2000 security information, see http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

About Microsoft Business Solutions

Microsoft Business Solutions, a division of Microsoft, offers a wide range of integrated, end-to-end business applications and services designed to help small, midmarket and corporate businesses become more connected with customers, employees, partners and suppliers. Microsoft Business Solutions' applications optimize strategic business processes across financial management, analytics, human resources management, project management, customer relationship management, field service management, supply chain management, e-commerce, manufacturing and retail management. The applications are designed to provide insight to help customers achieve business success. More information about Microsoft Business Solutions can be found at http://www.microsoft.com/BusinessSolutions/