Secure Software

Microsoft Dynamics® NAV 2009

Security Hardening Guide

White Paper

Microsoft Dynamics

Table of Contents

Introduction **4**

Microsoft Dynamics NAV 2009 Security Best Practices **5**

Secure Access to SQL Server 5
Secure Access to the C/SIDE Database Server 8
Security Considerations for Other Microsoft Dynamics NAV 2009 Components 8
NAV Server 8
Application Server for Microsoft Dynamics NAV 2009 9
Dynamics NAV Employee Portal 9
Commerce Gateway 9
Automated Data Capture System 9
Business Applications 11
Passwords and Database Access 12
Backups 12
Operating System and Updates 12
License Files 12
Recovery Plan 13

Physical Security **14**

Employees 14
The Administrator 14

Securing the Server Operating System **16**

Authentication 16
Strong Passwords 17
Defining a Password Policy 17
Defining an Account Lockout Policy 18
Access Control 18
Permissions 18
Ownership of Objects 18
Inheritance of Permissions 19
User Rights 19
Object Auditing 19
Access Control Best Practices 19

External Security Firewall **20**

ISA Server 2006 20
ISA Server Policies 20

Virus Protection **22**

Types of Viruses 22
Boot-Sector Viruses 22
File-Infecting Viruses 22

Trojan Horse Programs 22
Virus Protection Best Practices 23

Network Security Strategies 24
Wireless Networks 25
Network Security Scenarios 25
No Firewall 25
One Simple Firewall 26
One Existing Firewall 27
Two Existing Firewalls 27

Managing Security Updates 29

SQL Server Security Settings 31

Disclaimers 32

Introduction

Microsoft® provides operating systems with 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 your 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 only 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 easy for users or they will find less secure ways of doing things.

Note: This guide discusses security in the sense of preventing attacks on software components interacting over a network. Another type of security in Microsoft Dynamics NAV 2009 involves creating and maintaining users and roles. For information about this kind of security, run the Microsoft Dynamics NAV 2009 Classic client, open the online Help system, and view topics under 'Security and Permissions' in the Table of Contents.

Microsoft Dynamics NAV 2009 Security Best Practices

This section describes practices you should adopt when you are running Microsoft Dynamics™ NAV 2009. Following the guidelines in this document can help you increase the security of your Microsoft Dynamics NAV 2009 environment.

Note: One obvious and important best practice is that you should always run Microsoft Dynamics NAV 2009 on your corporate intranet, and not on the public Internet.

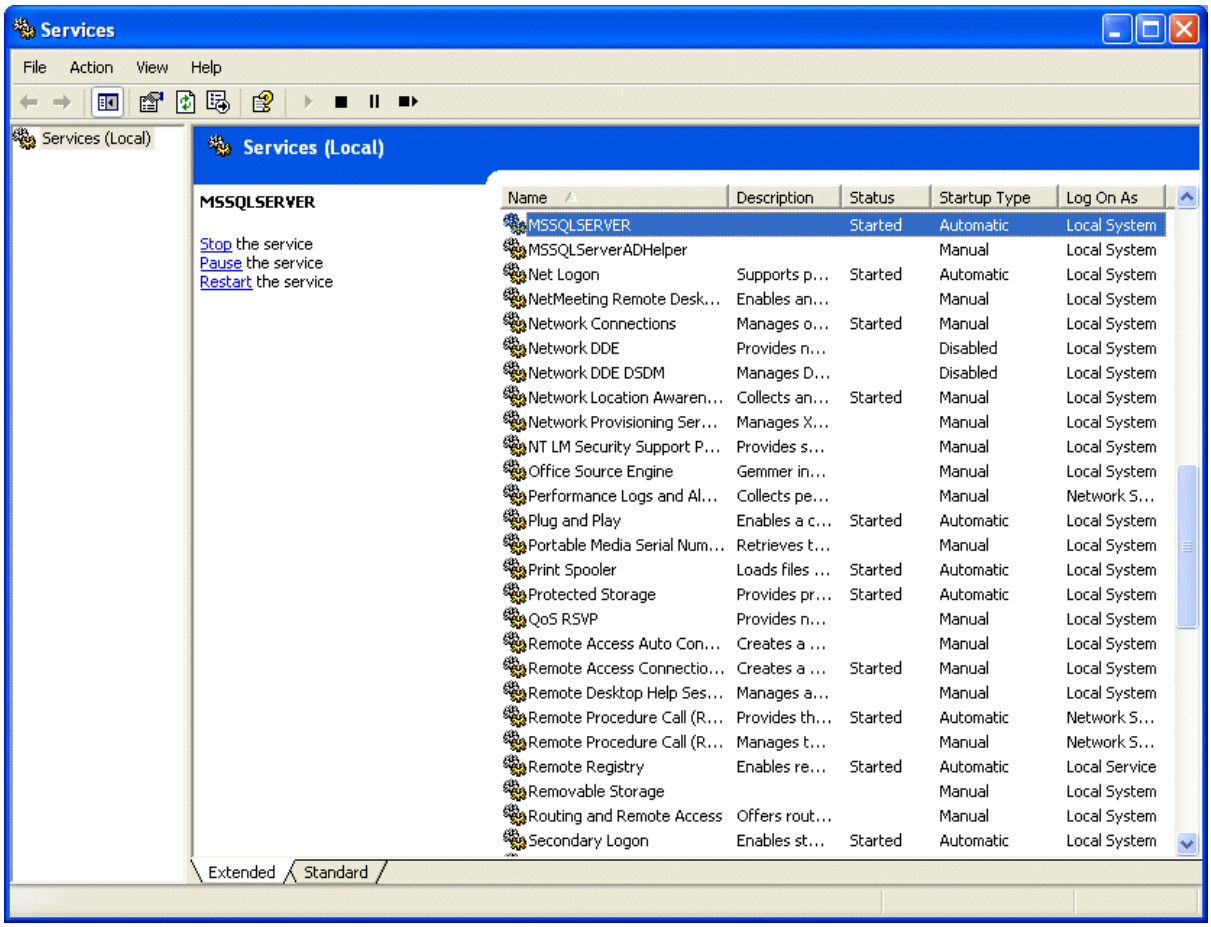
Microsoft Dynamics NAV 2009 can use either Microsoft® SQL Server® or the proprietary C/SIDE database server as its database server. Microsoft recommends that you run Windows Server™ 2008 or Windows Server 2003 R2 on the computer that hosts the database server. You can also use Windows Vista™ or Windows™ XP with smaller installations.

Secure Access to SQL Server

If you are running Microsoft Dynamics NAV with SQL Server, SQL Server runs as a Windows service. By default the SQL Server service uses the Local System account. Microsoft recommends that you do not use the Network Service account for the SQL Server or the SQL Server Agent services. Local User or Domain User accounts are more appropriate for these SQL Server services.

To view or change the account that SQL Server service is using, follow these steps:

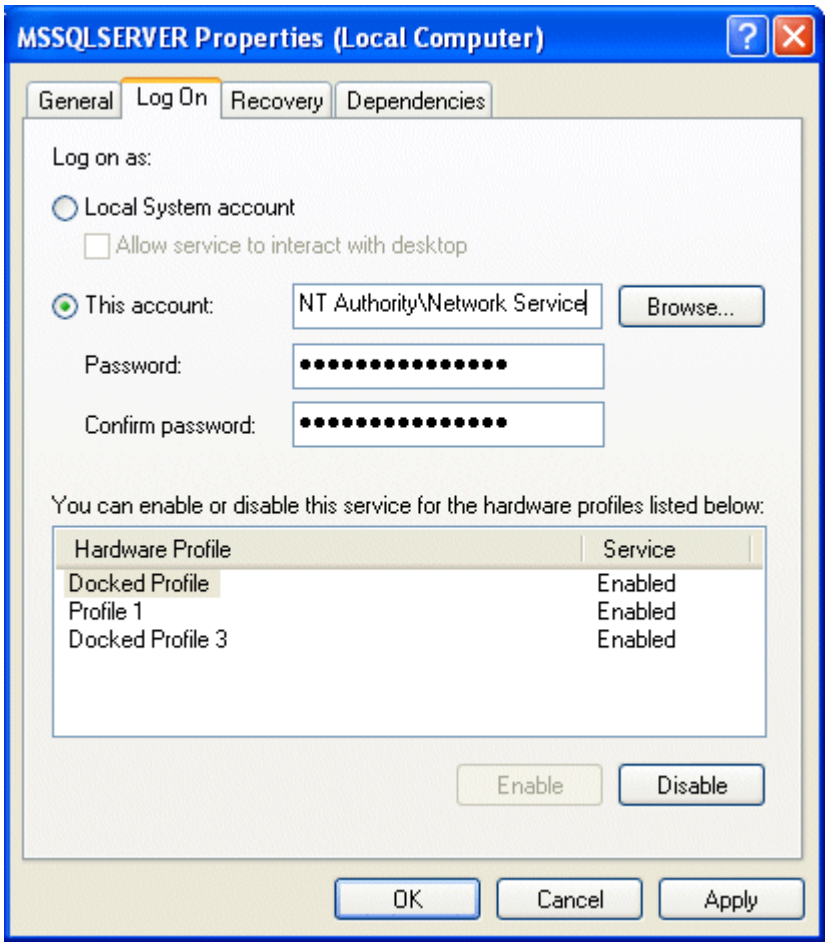
1. On the SQL Server computer, click Start, click Control Panel, double-click Administrative Tools, and then double-click Services to open the ***Services*** window.



Services window

2. Scroll down and select the service. If there is only one instance of SQL Server, the service is named "SQL Server (MSSQLSERVER)".
3. Right-click the service and select Properties to open the ***Properties*** tab.

4. In the ***Properties*** window, click the ***Log On*** tab.



SQL Server Service Properties window

5. In the ***Log On*** tab, under **Log on as**, select **This Account** and type (or confirm) the name of the account that you want to use for SQL Server service. If necessary, provide the appropriate password.
6. Click OK.

To ensure that users can connect to the database, you **must** give the specified account read/write permission to the database files. Follow these steps:

1. Open Windows Explorer and navigate to the folder that contains the database file.
2. Select the database file, right-click it, and click Properties.
3. In the ***Properties*** window, click the ***Security*** tab, and under **Group or user names,** click Add.
4. In the ***Select Users, Computers, or Groups*** window, enter the account name and click OK. The account is now in the list of **Group and user names** in the ***Properties*** window.
5. Select the account and, in the **Permissions** area, give it read/write permission.

For more information about security, see SQL Server Security. Also see Microsoft TechNet for further security guidance for SQL Server.

Secure Access to the C/SIDE Database Server

Microsoft recommends that you use the TCPS secure protocol for communications between Microsoft Dynamics NAV 2009 clients and the C/SIDE 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, the default protocol for the C/SIDE database server, is a strict protocol and only allows users to log on to the C/SIDE database server if the following criteria are met:

- The user's computer is in the same domain as the server.
- The user account is a Windows domain account in the same domain as the server and has been assigned one or more roles in the database.

If you are not using TCPS, Microsoft recommends that you create an account with least privileges for the service, having at most the same privileges as a normal Users account, or use a domain account that is not an administrator either in the domain or on any local computer. Give this account read/write access to the database files to ensure that the users can connect to the database. For more information about specifying access to files, see the preceding section, "Secure Access to SQL Server".

When you are running the C/SIDE database server as a service on the server computer, you **must** run the service as the *NT Authority\Network Service* account (on Windows Vista this account is called *Network Service*) or the Local System account. This means that you cannot run the server from a command prompt if you are using TCPS as the network protocol. For information about how to specify the log on account for a Windows service, see the preceding section, "Secure Access to SQL Server"..

Security Considerations for Other Microsoft Dynamics NAV 2009 Components

NAV Server

The new Microsoft Dynamics NAV Server is a .NET-based Windows Service application that works exclusively with SQL Server databases. The NAV Server provides an additional layer of security between the clients and the database. It leverages the authentication features of the Windows Communications Framework to provide another layer of user authentication and uses impersonation to ensure that business logic is executed in a process that has been instantiated by the user who submitted the request. This means that authorization and logging of user requests is still performed on a per-user basis. This ensures that all Windows authentication and Microsoft Dynamics NAV 2009 roles and permissions that have been granted to the user are correct. It also ensures that business logic–level auditing is still performed.

The NAV Server is a Windows service that runs as the NT Authority\Network Service account by default. This allows access a local SQL Server database. However, on a network you must ensure that the NAV Server service is running as a Windows domain account that is recognized by the SQL Server service. This account should not be an administrator either in the domain or on any local computer.

Client users can send files to be stored on the NAV Server, so Microsoft advises administrators to set up Disk Quotas on all NAV Server computers. Disk Quotas track and control disk space usage for NTFS volumes, allowing administrators to control the amount of data that each user can store on a specific NTFS volume. For more information about Disk Quotas, see the Disk Quotas Technical Reference on Microsoft TechNet.

Application Server for Microsoft Dynamics NAV 2009

The Dynamics NAV Application Server is a Windows service that runs as the NT Authority\Network Service account by default. This allows it to access the C/SIDE database server locally. However, on a network you must ensure that the Dynamics NAV Application Server service is running as a Windows domain account that is recognized by the C/SIDE database server. This account should not be an administrator either in the domain or on any local computer.

Dynamics NAV Employee Portal

If you are running Dynamics NAV Employee Portal, Microsoft recommends that you use HTTPS as the network protocol for your NEP installation to obtain a higher level security. HTTPS (HyperText Transport Protocol Secure) is a protocol for accessing a secure Web server. Using "HTTPS" in a URL instead of HTTP directs the message to a secure port number rather than the default Web port (80). Under HTTPS, sessions are managed by a security protocol such as SSL.

Commerce Gateway

Consider the following options for enhancing secure communications between Microsoft Dynamics NAV 2009 and the BizTalk Server.

Enable Commerce Gateway Security

Edit the TCPCom_Config.xml file to define the list of IP addresses that are allowed to communicate with the Commerce Gateway, and to encrypt data communications. Microsoft Dynamics NAV 2009 Setup installs TCPCom_Config.xml in the Commerce Gateway Broker directory within your Microsoft Dynamics NAV installation. To define the list of allowed IP address, follow these steps:

1. Change the value of the AllowAll parameter from Yes to No.
2. Create a separate AllowedId entry for each allowed IP Address.

You can also set the Cryptography parameter to Yes or specify that you want TCPCom to encrypt documents moving through the Commerce Gateway. All messages are encrypted using a symmetric key, and symmetric keys are exchanged using asymmetric keys.

Use Internet Protocol Security to Encrypt Network Traffic

Internet Protocol security (IPsec) is a framework of open standards for protecting communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPsec is based on standards developed by the Internet Engineering Task Force (IETF) IPsec working group.

IPsec is supported by the Microsoft Windows Vista, Windows Server 2008, Windows Server 2003, and Windows XP operating systems and is integrated with the Active Directory directory service. IPsec policies can be assigned through Group Policy, which allows IPsec settings to be configured at the domain, site, or organizational unit level.

Place the IIS Server Behind a Firewall

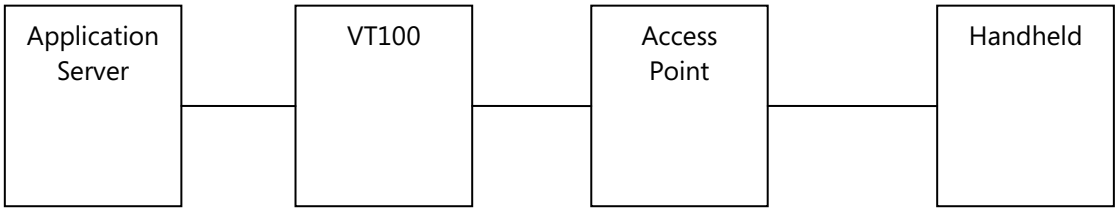
For more information, see the section on External Firewall Security, later in this manual.

Automated Data Capture System

The Automated Data Capture Systems (ADCS) is a NAV tool that gives companies the ability to accurately capture data for inbound, outbound, and internal documents, primarily in connection with

warehouse activities. With ADCS, company employees using handheld devices and radio frequency technology can continuously validate warehouse inventories.

These are the components in an ADCS installation.



All components communicate using TCP sockets.

The following subsections explain the connections between the respective components.

Microsoft Dynamics NAV Application Server to VT100

Communication between these components is based on TCP sockets. The communicator initiator is the VT100 Plug-in sending an XML document to the NAV Application Server, requesting processing. The result is then embedded in the same XML document.

It is not required to have the Microsoft Dynamics NAV Application Server and the VT100 service on the same host computer, but in lieu of encryption, it is the safest and fastest configuration. Microsoft Dynamics NAV 2009 communication between these two components is encrypted. To learn how to set up the system, see the ADCS manual for Microsoft Dynamics NAV 2009.

VT100 to Access Point

In a strict sense, the Access Point only works as a communication node between the handheld and the VT100 Plug-in, but physically it is a different piece of hardware handling the connection. Care should be taken to secure communications on both sides of the Access Point (to the VT100 Plug-in and to handhelds).

To secure the connection from the VT100 Plug-in to the Access point, Microsoft recommends hard-wiring the Access Point directly to the computer where the VT100 service is hosted, as the communication between these devices not encrypted (VT100 protocol). It is possible to connect both the Access Point and the VT100 in a network, but this can create security flaws. If you do connect the hardware directly, also verify that the VT100 Plug-in port is accessible only from the corresponding network hardware.

Access Point to Handheld

Usually this communication is wireless, so if the hardware allows it, it should be encrypted. For information about how to enable encryption between these components, see the manual for the respective Handheld and Access Point hardware.

Securing Your System

All data that is displayed and entered in your handheld is transported to all involved systems, so the goal is to prevent sniffers and "middle-men" attacks. Use encryption to minimize the risk of data availability through opened networks.

Each connection has its own vulnerability, so you should secure each connection point and data transfer, as discussed earlier. You can install your database server on one computer, your Microsoft Dynamics NAV Application Server on another computer, and the VT100 on yet another computer, but since all of these connections transfer data differently using different technologies, not all deployments will be as safe as others.

Ideally, you should have a single computer containing all the components in the same computer with the Access Point hardwired to it. Since most installations do not allow this configuration, you should take advantage of the encryption available between the Microsoft Dynamics NAV Application Server and the VT100 Plug-in to deploy split systems.

If you are using the encrypted ADCS available in Microsoft Dynamics NAV 2009, we recommend the following configuration:

- Microsoft Dynamics NAV database on one computer.
- Microsoft Dynamics NAV Application Server on another computer, communicating with the database.
- Computer hosting the VT100 Plug-in service located closest to the handhelds, with the Access Point hardwired to this computer. Configure your external firewall to allow connections only to the VT100 Plug-in through this network interface.
- Use the strongest available wireless encryption for both the Access Point and the handheld.

Business Applications

Be sure that all Microsoft Dynamics NAV C/SIDE applications you install have been built, reviewed, and delivered by a trusted party. Take care to review all applications for security and privacy.

Since the Role Tailored client can upload and download files to the NAV Server, application logic should be resilient to malicious files that could be sent to the server. Enforce file quotas and size restrictions on users so that uploaded files from the client cannot unexpectedly fill the server hard disk. Take care to not show server file path information directly on RoleTailored client forms or in error messages.

New applications should not store or access passwords. But if you have legacy applications or applications that require password storage, follow these guidelines:

- Avoid using masked fields on forms to store passwords. These fields may not be visible to users but they might be visible in a report. And they are not encrypted in the database when stored.
- If possible, try to use a public/private certificate system. Certificate storage is built into the Windows operating systems and is documented in the Cryptography Functions section of MSDN, under "Certificate and Certificate Store Functions."
- If passwords are required in the application, try to avoid storing them directly in the database. You can use a separate Com component to maintain passwords.

Passwords and Database Access

Always use strong passwords. For more information about strong passwords, see the "Strong Passwords" section (under "Securing the Server Operating System").

Do not reuse passwords. 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 domain that use the same password, and even set local administrator passwords on domain computers that are the same across the domain. In this situation, if a single account or computer is compromised, the entire domain is compromised.

After Microsoft Dynamics NAV 2009 is installed and the database has been attached, you should create a Windows Login for your database administrator and assign this login the SUPER role in Microsoft Dynamics NAV. This SUPER user then manages tasks such as database administration and security. Only those users who need to perform these kinds of administrative tasks should be granted the SUPER role in Microsoft Dynamics NAV.

All other users accessing the Microsoft Dynamics NAV database should run with least privilege. This means assigning user roles in Dynamics NAV that give access only 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 or create and restore database backups.

Backups

Make regular backups of your Microsoft Dynamics NAV database and remember to test the backups to ensure that they can be restored successfully.

Store your backups in a safe place to secure them from theft and tampering and to limit the impact of hazards like fire, smoke, dust, high temperature, lightning, or major environmental disasters such as an earthquake. When the backup is in a different geographical location than the server, it eliminates the chance that the same incident could destroy both the server and the backup.

Note: Database access in Microsoft Dynamics NAV 2009 requires authentication with user name and password. However, a person restoring a backed-up database is able to open that database without authentication. For this reason, always restrict physical access to database backups.

Operating System and Updates

Although Microsoft Dynamics NAV can run on any recent version of Windows, we recommend that you use the newest operating systems with the most up-to-date security features. This is currently Windows Server 2008 or Windows Vista.

Use the Windows Update service provided by Microsoft to apply the most recent security updates. And use the Automatic Update feature of Windows to keep all your client computers up to date with the most recent security updates and service packs.

License Files

If you are using SQL Server as your database server, your license is stored in a system table on the server, and is protected by standard SQL user access control. If you are using the C/SIDE database

server, the license file is stored on the server computer in the runtime/installation directory. Be sure access to this directory is limited.

Keep the original media on which the license file is supplied in a secure location where it cannot be tampered with or stolen.

Recovery Plan

You should have a disaster recovery plan that ensures the rapid resumption of services after a disaster. A recovery plan should address issues such as:

- Acquiring new or temporary equipment to replace damaged or lost equipment.
- Restoring backups onto new systems.
- Testing that your 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. With this in mind you should:

- Keep unauthorized users away from the computers.
- Ensure that burglar alarms, access security features such as cardkey readers, and surveillance features are in place.
- Ensure that backups of critical data are stored offsite in fireproof containers.

Employees

It is a good policy to limit administrative rights across all products and features. As a default, employers should give their employees no more than read access to system functions, unless certain employees require greater access to perform their jobs. Microsoft suggests following the principle of least privilege: give users only the minimum privileges they require to access data and functionality.

Disgruntled and former employees are a potential threat to network security. With this in mind you should:

- Conduct pre-employment background investigations.
- Protect yourself against any potential actions by disgruntled employees and former employees.
- Ensure that you disable all Windows accounts and passwords when an employee leaves the company. 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.
- Be 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

System administrators are advised to 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 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 locate valuable information and identify best practices.

The more complex your network, the more difficult it will be to secure or fix the breach once an intruder has successfully gained access. Administrators should document the network topography thoroughly, with the aim of keeping it as simple as possible.

Security is primarily a matter of risk management. Because technology is not a cure-all, security requires a combination of technology and policy. There will never be a product that you can simply unpack and install on the network that instantly assures perfect security. 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 administrators can determine the right policies for each organization. Be sure to plan for security early in the implementation and deployment process. Understand what you want to protect and what you are willing to do to protect it.

Finally, develop contingency plans for emergencies before they happen. The combination of thorough planning with solid technology provides the greatest security.

For more information about security, see "The Ten Immutable Laws of Security Administration". Also, refer to the articles on security management in the column archive at Microsoft Technet – Viewpoint.

Securing the Server Operating System

Although many smaller customers do not have a server operating system, it is important to understand the security best practices that apply 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 even if you only have client operating systems.

The concepts in this section apply to Microsoft Windows Server 2008 and Windows Server 2003. Windows Server 2008 offers a robust set of security features, and the Online Help for Windows Server 2008 contains complete information about all the security features and procedures.

For additional information about Windows Server 2008, see Windows Server TechCenter. Information is also available at TechNet for Windows Server 2003.

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 using 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 resources based on the user's identity and membership in various predefined groups. Access control is typically used by system administrators for controlling access to network resources such as servers, directories, and files. The administrators typically grant users and groups permission to access specific objects.
- Single sign-on is a technology that allows a user to log on to the Windows domain once, using a single password, and automatically be authenticated 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 about these three key features.

Authentication

Authentication is a fundamental aspect of system security and confirms the identity of any user trying to log on to a domain or access network resources. The weakest 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. We recommend the following password best practices:

- Always use strong passwords.
- If passwords must be written 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 a network is often underestimated and overlooked. You should therefore instruct or even require your employees to use strong passwords.

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

For guidelines on creating strong passwords that the user can remember, see Strong passwords: How to create and use them.

Defining a Password Policy

When you are defining your password policy, be sure to create a policy that requires all the user accounts have strong passwords. For most systems, following the recommendations in the Windows Server 2008 Security Guide is sufficient:

- Define the **Enforce password history** policy setting so that several previous passwords are remembered. With this policy setting, users cannot revert to a recent 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 former passwords. Users must wait the specified number of days to change their passwords.
  Recommended setting: 2

- Define a **Minimum password length** policy setting. Longer passwords, of eight or more characters, are stronger than shorter ones. With this policy setting, users cannot use blank or one-character passwords.
  Recommended setting: 8

- Enable the **Password must meet complexity requirements** policy setting. This setting ensures that passwords have at least three symbols from the four categories (uppercase letters, lowercase letters, numbers, and non-alphanumeric symbols), and that they do not contain any portion of a user's name. Recommended setting: Yes
- **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

Note: Keep in mind that a password can meet all these requirements and still not be very strong. For example, “Password1” meets these requirements.

For a full list of password requirements, see "Password Must Meet Complexity Requirements" in Windows Server Online Help.

Defining an Account Lockout Policy

Be cautious when defining the account lockout policy. In a small business it is unwise to use an account lockout policy as it is likely to lock out authorized users, which can be very costly.

If you decide to apply an account lockout policy, set **Account lockout threshold policy** to a high number so that authorized users are not locked out 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 Microsoft Dynamics NAV 2009) can be effectively secured after a consideration of what rights users, groups, and other computers are to have on the network. You can secure a computer or network 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 can be granted to any user, group, or computer. It is a good practice to manage permissions through groups.

Ownership of Objects

When a member of the Administrators group creates an object in Windows Server 2003 or Windows Server 2008, 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 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 permissions so designated are inherited.

User Rights

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

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

Object Auditing

You can audit users' access to objects and 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

Try to comply with the following guidelines when setting up and maintaining user and group permissions:

- 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 administrators. A better solution is to remove the Everyone group, and to give users, groups, or computers permissions to an object. Remember that if no permissions are defined, 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 subtree of a parent object. By doing this, you gain the greatest effect with the least effort. The permission settings that 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, be 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 2008 Online Help.

External Security Firewall

A firewall is hardware or software that can prevent 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 the following 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 contained in the packet.
- The port number to which the packet 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 (R2) ships with Microsoft Internet Security and Acceleration (ISA) Server 2004 as its firewall solution. Small Business Server Standard Edition also includes a firewall. Microsoft Windows Small Business Server 2008 is scheduled for release in the second half of 2008.

ISA Server 2006

Internet Security and Acceleration (ISA) Server 2006 securely routes requests and responses between the Internet and client computers on the internal network.

The 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 being accessed interprets the requests from the ISA Server computer as if they originated from the client application.

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

The 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 the 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 the ISA Server and IIS ports, 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 that you use antivirus software on all your computers.

Virus software is usually installed at each of these three locations: 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, and 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 this program is run, it can destroy or scramble data.

Virus Protection Best Practices

The spread of viruses can be prevented. Here are some guidelines for avoiding infection:

- 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 you feel is trustworthy.
- Talk to the person who created the document. If recipients are at all unsure whether a document is safe, they should contact the person who created the document.
- Use 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).
-

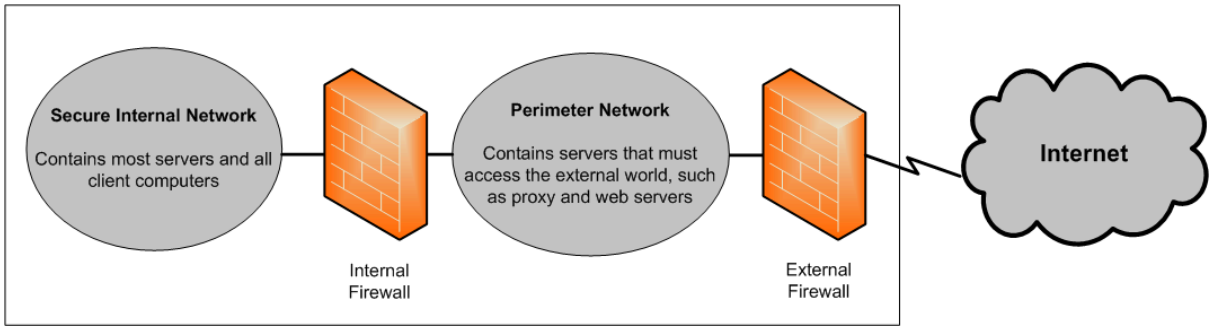
For more information about viruses and computer security, visit:

- Microsoft Security at Security Central
- Security on Microsoft TechNet

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 factor in safeguarding network integrity. A firewall is not a single component, but rather a system or combination of systems that enforces a boundary between two or more networks. Although different terms are used, the boundary between networks 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 to secure the private network.



Organizations vary in their approach to using firewalls for providing security. The following list details some common approaches.

- **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. Overall, IP packet filtering offers weak security, is cumbersome to manage, and is easily defeated.

- **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. Overall, 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**

  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 used 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. Overall, circuit gateways are most effective when the user of a network application is of greater concern than the data being passed by that application.

- **Proxy Servers**
  Proxy servers are comprehensive security tools that provide firewall and application gateway functionality to 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. Overall, proxy servers are a comprehensive security tool that includes an application gateway, safe access for anonymous users, and other services.

Be sure to take advantage of these firewall security features. 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 your needs and 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 2006.

For more information about TCP/IP, see "Designing a TCP/IP Network".

Wireless Networks

Wireless networks are typically configured in a manner that allows eavesdropping on the wireless signals. These networks 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 vulnerablef 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 also include a firewall to protect the computers from unwanted intruders on the Internet.

For more information about protecting a wireless network, see Securing Wireless LANs with PEAP and Passwords.

Network Security Scenarios

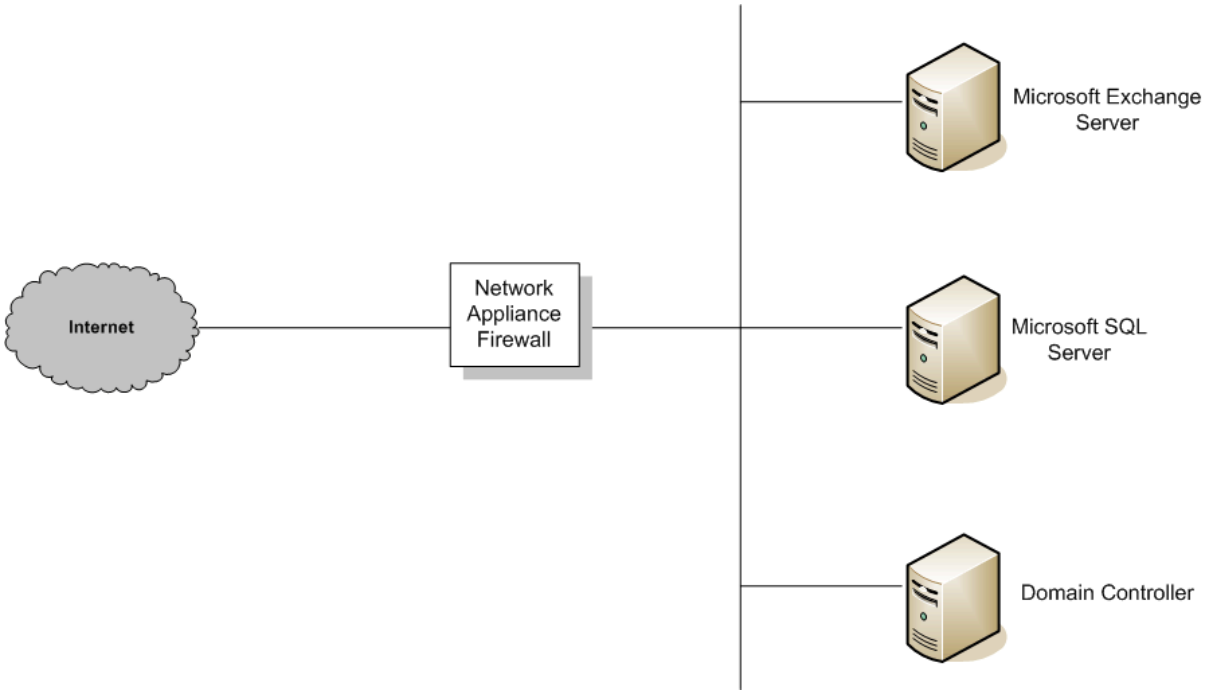
The level of network security that your organization requires depends on several factors that are oftentimes a compromise between budget and the need to keep the corporate data safe. It is possible for a small business to have a very complex security structure that provides the highest possible level of network security, but a small business may not be able to afford that level of security. In this section, there are four scenarios, which illustrate varying levels of network security.

No Firewall

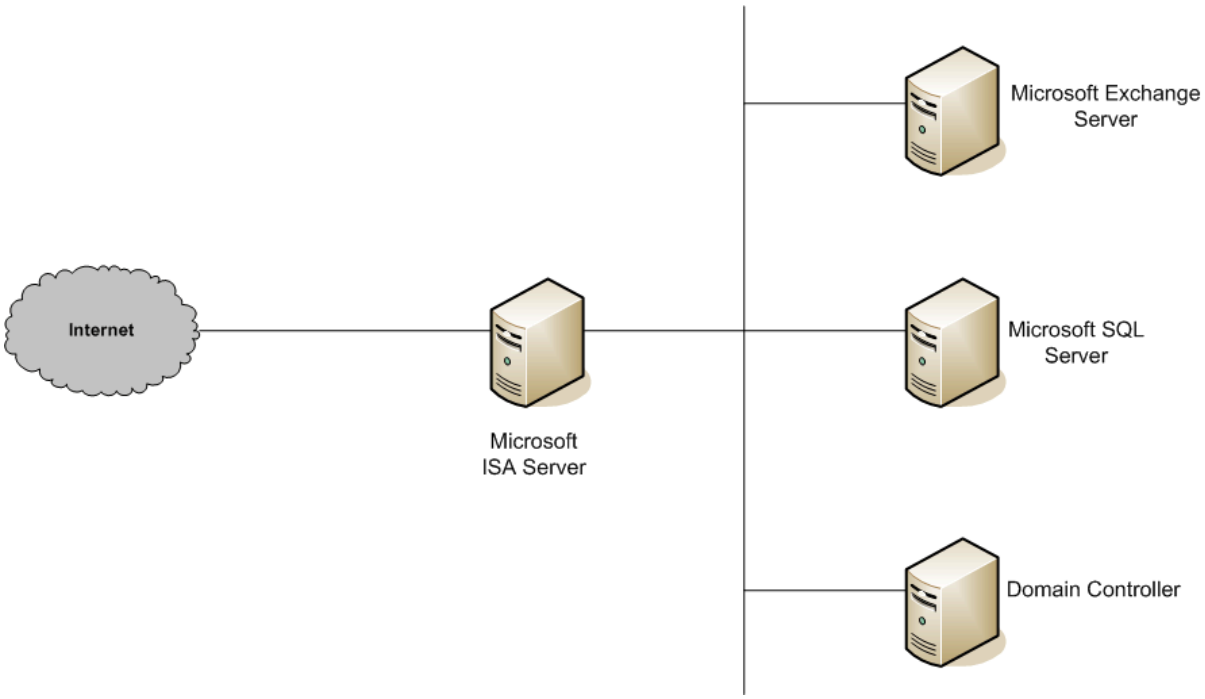
If you have a connection to the Internet but no firewall, some measure of network security needs to be implemented. There are simple network firewall appliances that provide enough security to deter most would-be hackers.

One Simple Firewall

The minimum level of security recommended is a single firewall between the Internet and your data. This firewall may not provide any level of advanced security and should not be considered very secure.



Hopefully, your budget allows a more secure solution that will protect your data. One such solution is ISA Server 2006. The increased cost of this additional server provides a great deal more security than your average consumer firewall, which typically only provides network address translation (NAT) and packet filtering.



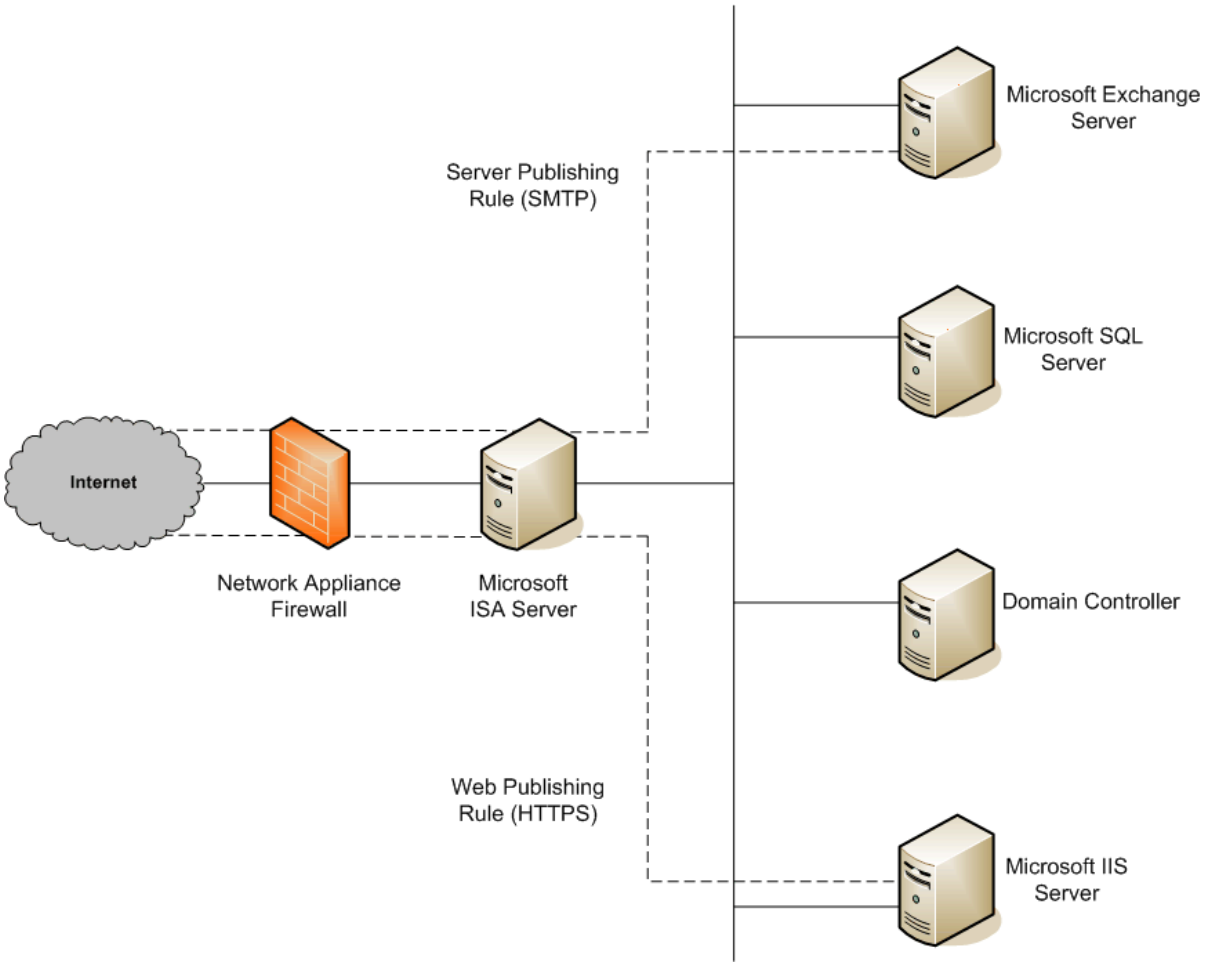
This single firewall solution is more secure than an entry level firewall appliance and provides Windows–specific security services.

One Existing Firewall

If you have an existing firewall that separates your intranet from the Internet, you may want to consider an additional firewall that offers 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, an ISA Server can impersonate a Web server to the outside world, fulfilling client requests for Web content from its cache. The ISA Server forwards requests to the Web server only when the requests cannot be served from its cache.

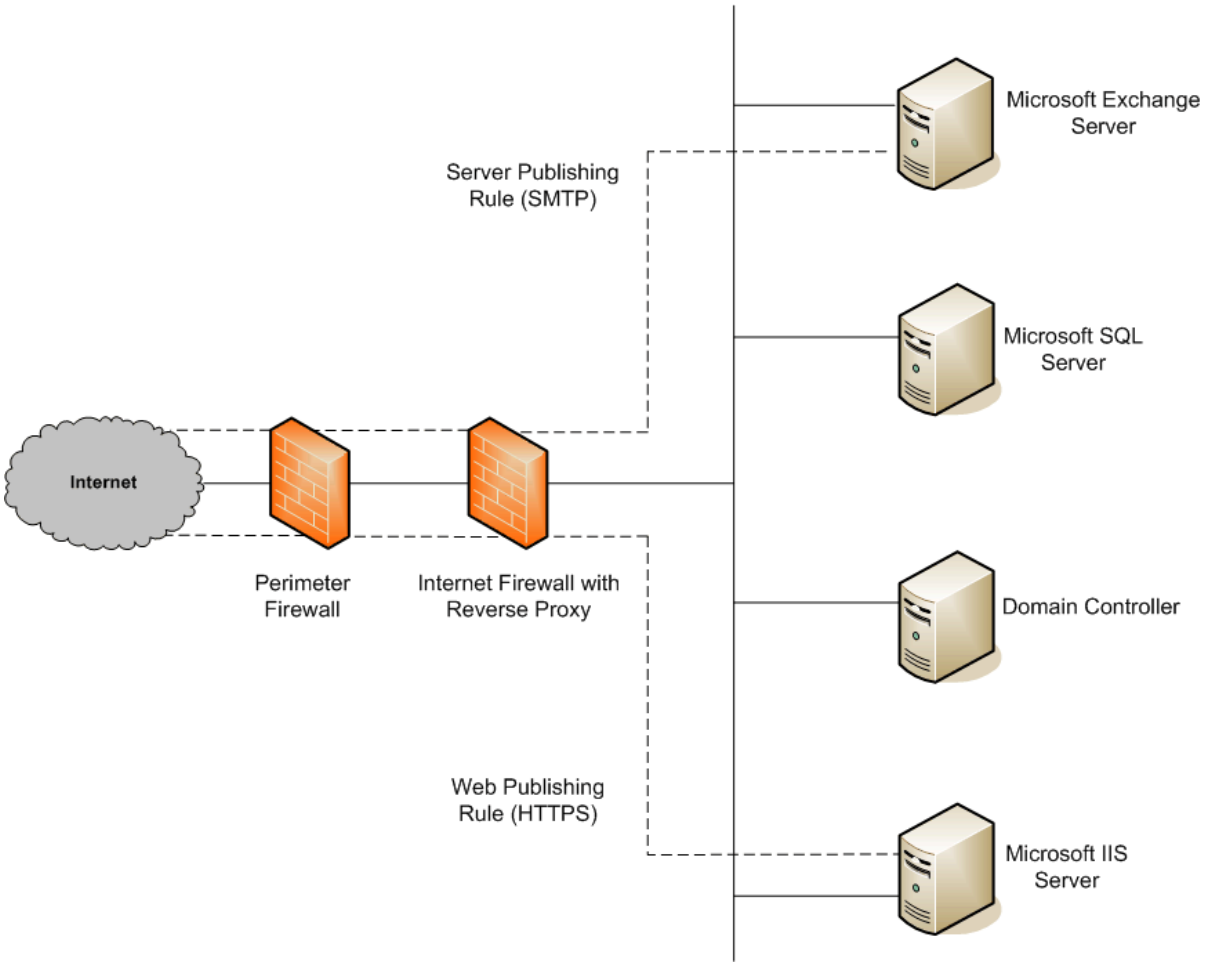
Another method is server publishing. The ISA Server allows the publishing of internal servers to the Internet without compromising the security of the internal network. You can configure Web publishing and server publishing rules that determine which requests should be sent to a server on the local network,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



Two Existing Firewalls

The fourth scenario is where the organization has two firewalls in place with an established perimeter network. One or more servers provide 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.



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.

Managing Security Updates

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, update management is a large part of the overall change and configuration management strategy. Whatever the nature and size of the organization, it is vital to have a good update management strategy, even if the organization does not yet have effective change and configuration management in place. The vast majority of successful computer system attacks are against systems where security updates have not been installed.

Security updates present a 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 Microsoft software, Microsoft strives to release a security update as soon as possible. Until the update is deployed, the security that the client depends upon may be severely diminished.

In the Microsoft Dynamics NAV environment, you must ensure that your clients have the most recent security updates installed throughout their system. Be 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 TechNet Product Security Notification.

- Microsoft Automatic Updates
  Windows can automatically apply security updates to your computers.

- Microsoft Security Bulletin Search Tool
  The Security Bulletin search tool is available at Security Bulletin Search. Clients can determine which updates they need based on their current operating system, applications, and service packs.

- Microsoft Baseline Security Analyzer (MBSA)
  This graphical tool is available at Microsoft Baseline Security Analyzer. 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, Exchange, and Exchange Server.

- Microsoft Systems Management Server (SMS) Software Update Services Feature Pack
  The SMS Software Update Services Feature Pack contains tools for easing the process of distributing software updates throughout your company. These 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 Software Update Services Feature Pack.

You should consider using each of these tools. It is very important that you address security issues as quickly as possible, while maintaining the stability of your environment.

SQL Server Security Settings

Microsoft Dynamics NAV 2009 can run on SQL Server. Smaller installations can also run on SQL Server Express.

The following steps will help increase SQL Server security:

- Be sure that the latest operating system and SQL Server service packs and updates are installed. For the latest details, check Microsoft Security.

- For file system-level security, be sure all SQL Server data and system files are installed on NTFS partitions. Make the files accessible only to administrative or system-level users through NTFS permissions. This prevents users from accessing those files when the MSSQLSERVER service is not running.

- Use a low-privilege Local User or Domain User account for the SQL Server service (MSSQLSERVER or SQLEXPRESS). This account should have minimal rights in the domain and should help contain (but not stop) any attack to the server in case of compromise. This account should have only local user-level permissions in the domain. If SQL Server 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 Management Studio. The access control lists (ACLs) on files, the registry, and user rights are changed automatically.

- Avoid granting users special end-user privileges on the computer running SQL Server. Doing so would give such users direct access to the database server, thereby bypassing the Microsoft Dynamics NAV permission layer.

- Most editions of SQL Server are installed with some default databases. These are sample databases 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 an exploitation involving default settings and default configurations. If the sample databases are present on the production SQL Server computer, they should be removed.

- Auditing of the SQL Server 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 security information, visit the SQL Server Security Web site.

Disclaimers

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.