Security Considerations White Paper for Cisco Smart Storage

"An open network is like a bank's vault with windows" ... Bill Thomson

Network-Attached Storage (NAS) is a relatively simple and inexpensive way to provide file-based data storage services to other devices on the network. NAS can also be used to host web server, and other services (iTunes, MySQL, PHP, web DAV, etc.). NAS uses protocols such as SMB/CIFS (Server Message Block/ Common Internet File System), NFS (Network File System), AFP (Apple Filing Protocol), and FTP (File Transfer Protocol). It is managed by HTTP/HTTPS and can be accessed remotely via SSH (Secure Shell). Despite its flexibility and cost benefits, deploying NAS over IP networks potentially exposes customer data to security risks. Like everything else in the IP infrastructure, the NAS must be protected from security vulnerabilities such as Denial of Service (DoS) and other malware attacks. In addition, Elevation of Privileges can also occur if guest's account is not managed properly. These security risks can result in data being stolen, corrupted, and applications not functioning properly. Because of its broad capabilities, unique security considerations must be addressed when deploying the NAS in your network.

This document offers some security best practices and considerations when setting up the Cisco Smart Storage, so that these risks and vulnerabilities can be minimized. The following topics are included in this document:

Typical NAS Deployments in an IP Network

The following illustrations show the NAS in three typical deployments.

Figure 1 NAS in a DMZ (Direct Internet Connection) Deployment

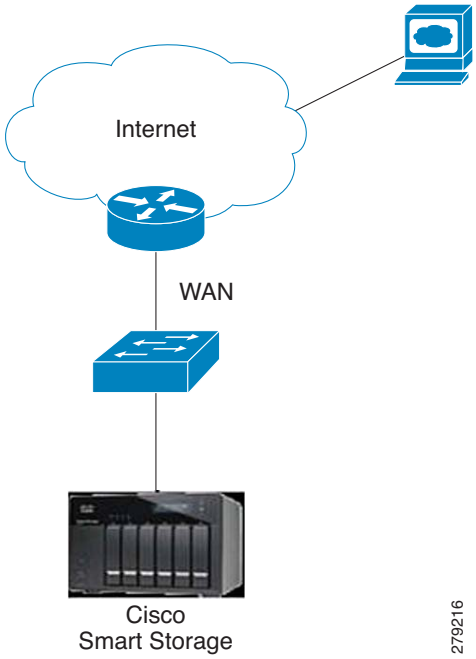


Figure 2 NAS in a LAN Deployment

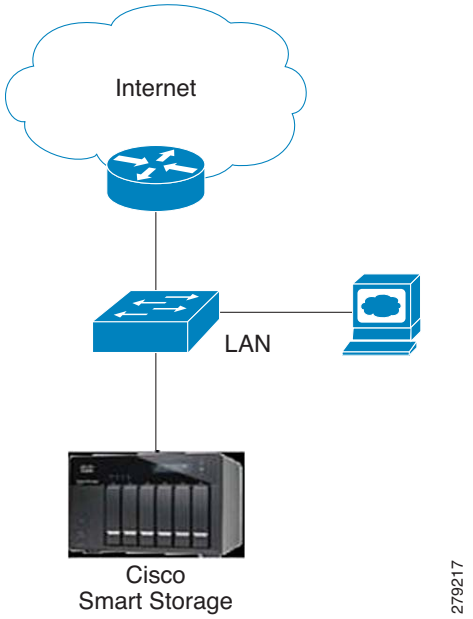
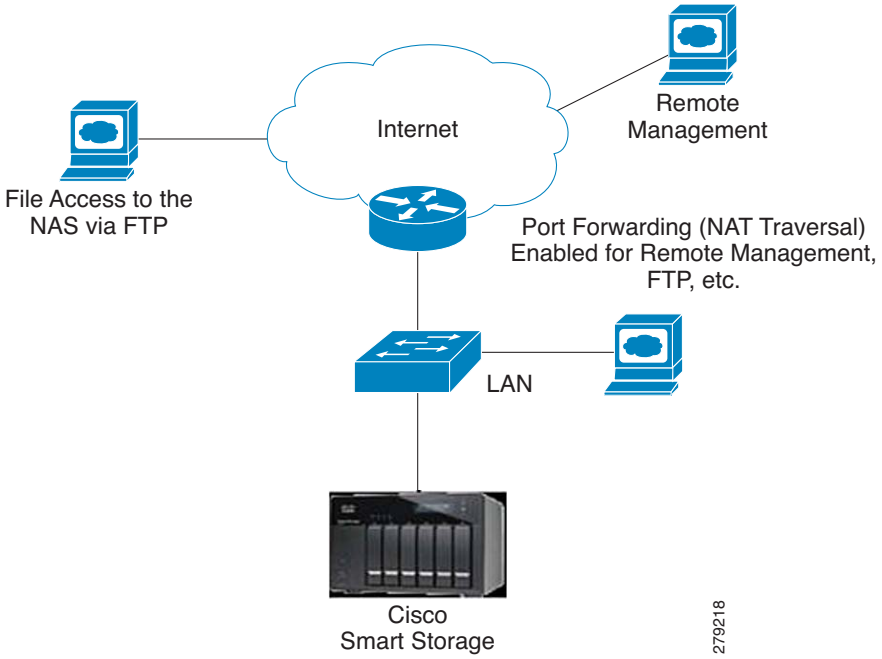


Figure 3 NAS in a WAN/LAN Deployment



Introduction

The NSS 300 Smart Storage is a very flexible network resource that can be deployed in various environments:

- NAS servicing the public Internet.
- NAS exclusively servicing a closed LAN.
- NAS providing services to the public Internet from behind a router, firewall or gateway.
- NAS providing application service protocols.

This section investigates several tools used to exploit security vulnerabilities in these various network environments.

Some background is provided on the following network and system tools and how they are used to put your network at risk:

Nessus	Nikto	Metasploit Framework	Nmap
Xprobe2	Amap	Winfo	Hping2
John the Ripper	THC Hydra		

To harden your business network, the following recommendations can be implemented to minimize exposure to these vulnerabilities:

- Enable Password Strength Enforcement
- Disable unused process, applications, guest accounts
- Deploy FTP over SSL
- Disable Anonymous FTP
- Enable Network Access Protection
- Deploy SNMPv3 instead of SNMPv2
- Deploy HTTPS for the administration functions
- Disable HTTP
- Deploy port forwarding from WAN to access LAN resources

- Deploy VPN instead of port forwarding
- Enable WiFi security with WPA2/AES
- Remove Local Group = everyone on USB/eSATA
- Monitor the appropriate NSS logs for suspect behavior
- Utilize ACL to limit physical access to storage resources

Details about security exploitation methodologies and best practices to prevent them can be found in detail in the next section, **Hacker's Tools and Exploitations for NAS**.

Hacker's Tools and Exploitations for NAS

These are some of the tools available for the hacker to use to exploit and identify security vulnerabilities for Network-attached storage. If the NAS is not properly secured, the end result can lead to loss of sensitive information (confidential company information, marketing strategies, etc.), correspondence (emails, contacts), or financial details. However, these risks can be minimized and the product can be secured by following the best security practices outlined in this document.

- **Tools to identify web server vulnerabilities:**
  - **Nessus**—A vulnerabilities scanning tool. Hacker utilizes this tool to determine potential vulnerabilities of the NAS. This tool lists all of the potential vulnerabilities of the NAS. For example, the Apache server patch is not up-to-date, the server uses weak SSL ciphers, etc.
  - **Nikto**—A web vulnerabilities scanner. This tool lists all of the potential security holes. For example, "OpenSSL/0.9.8e appears to be outdated (current version should be at least 0.9.8g)," etc.
  - **Metasploit Framework**—A vulnerability exploitation tool. It is an advanced open-source platform for developing, testing, and using exploit code.
- **Tools to identify open ports, services, and user accounts:**
  - **Nmap**—TCP/UDP ports scanning tool. Hacker utilizes this tool to determine open TCP/UDP ports on the device. For example, if FTP service is running on the NAS, the scan will indicate that TCP port 21 is open.

- **Xprobe2, Amap**—OS and application fingerprinting scanners. Hacker uses these tools to determine the version of the OS and the application version. Based on this information, the hacker can tailor the attack specific to the OS version or the application version.
- **Winfo**—Uses null sessions (guest account) to remotely retrieve information about user accounts, workstation/interdomain/server trust accounts, etc.
- **Hping2**—A network probing utility. It is like ping on steroids. This tool is particularly useful when trying to do a traceroute, ping, or probe of a host behind a firewall. This often allows you to map out firewall rule sets.

- **Tools to hack passwords:**
  - **John the Ripper**—A powerful, flexible, and fast multi-platform tool for cracking password hash. It's primary purpose is to detect weak UNIX passwords. It supports several crypt(3) password hash types which are most commonly found on various UNIX flavors, as well as Kerberos AFS and Windows NT/2000/XP hashes.
  - **THC Hydra**—A fast network authentication cracker. It can perform brute force attacks or rapid dictionary attacks against more than 30 protocols, including telnet, FTP, HTTP, HTTPS, SMB, etc. Figure 4 shows a log of an attacker's usage of known logins and passwords.

Figure 4 Log of Hacker Utilizes Hydra to Determine the Password

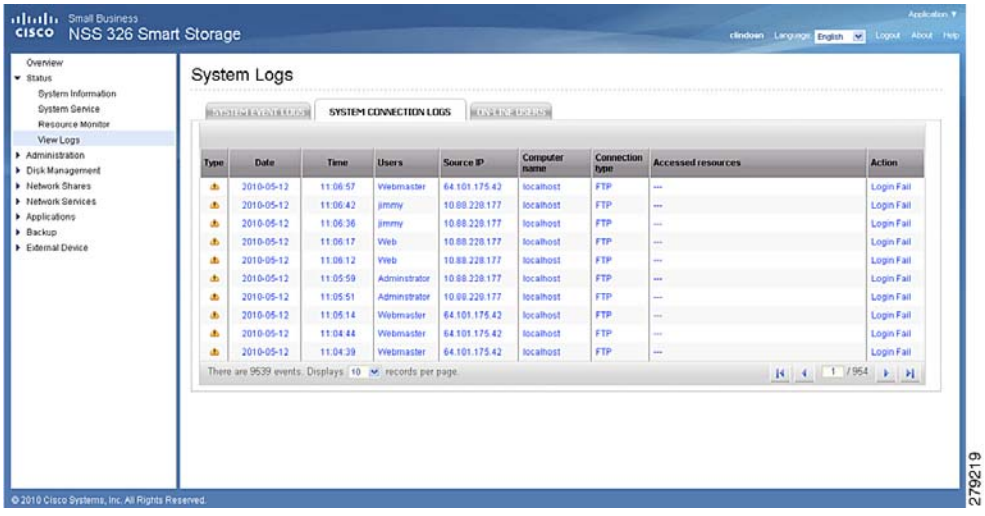
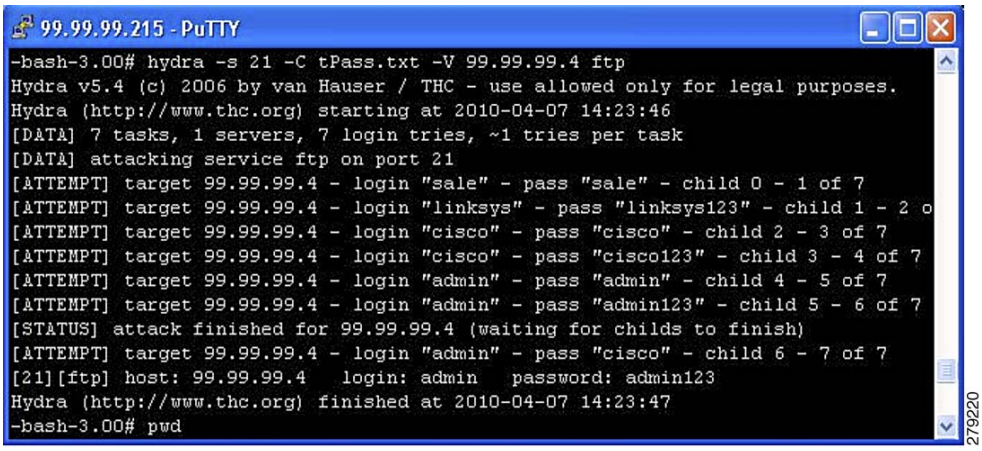


Figure 5 An Example of Hydra at Work (Hacking Password for FTP)



A typical network hack includes a user running a network scanning tool such as nmap to determine the open TCP/UDP ports. After the open TCP or UDP ports are identified, the hacker then runs the THC Hydra tool, using a list of known passwords or dictionary attacks method to determine the password. A more sophisticated hacker can utilize a tool such as “winfo” that can quickly scan the list of user accounts on the system (Figure 7) based on guest access. After determining the open ports and a list of user accounts, the hacker then customizes the attacks based on this information (i.e. brute force attacks or dictionary attacks to determine the passwords). It is almost impossible to prevent all of the possible attacks and make the system usable. However, by employing some of the security considerations outlined in Security Best Practices and Considerations, these vulnerabilities are minimized.

Security Best Practices and Considerations

Security Best Practices

The following is a list of best practices that help to safeguard the NAS from hackers. Some of these are deployment model specific. Please see Deployment Model Specific Security Considerations, page 12 for more information.

1. Enable Password Strength Enforcement—This makes it harder for the attacker to crack the password. The strong password should utilized these rules:

    a. The new password contains characters from at least three of the following classes: lower case letters, upper case letters, digits, and special characters.

    b. No character in the new password may be repeated more than three times consecutively.

    c. The new password must not be the same as the associated username or the username reversed.

    d. The new password must not be “cisco”, “ocsic”, or any variant obtained by changing the capitalization of letters therein, or by substituting “1” “|” or “!” for i, and/or substituting “0” for “o”, and/or substituting “$” for “s.”

For example, test123 or mom’s birthday are not strong passwords. A strong password should be something like “aM2z!nG6” or “ApD@th!nG.”

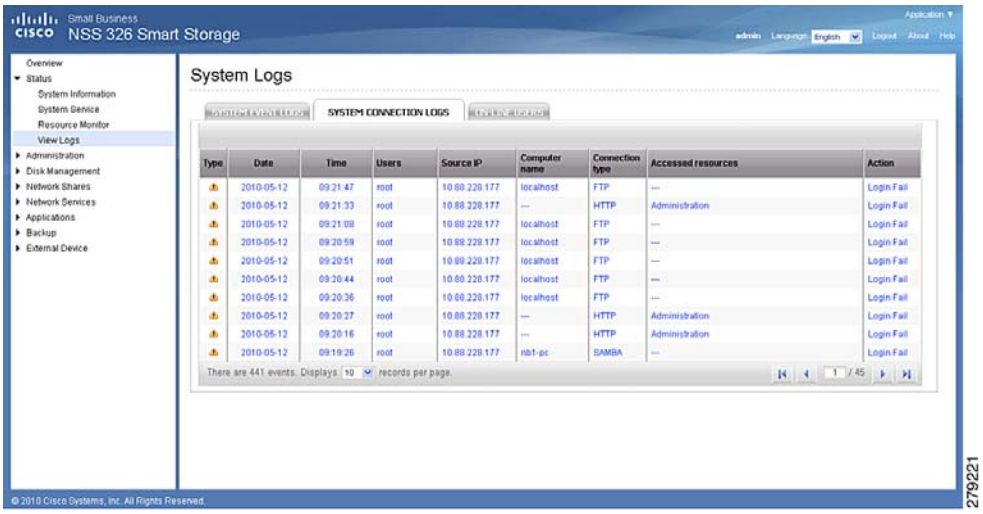
2. Turn off unused processes and applications. This will minimize the exposure to unnecessary security vulnerabilities. Currently, the NAS supports services and applications such as AFP (Apple Filing Protocol), telnet, SSH, SNMP, FTP, Web Server, Web File Manager, Multimedia Station, iTunes Service, and MySQL Server. For the user’s protection, with the exception of SSH and Web File Manager, these services and applications are disabled by default. The idea is to only enable services and applications on an as needed basis. Users who don’t need CLI access should disable SSH too.

3. Use FTPS instead of FTP—FTP over SSL is more secure than FTP.

4. Turn off Anonymous FTP.

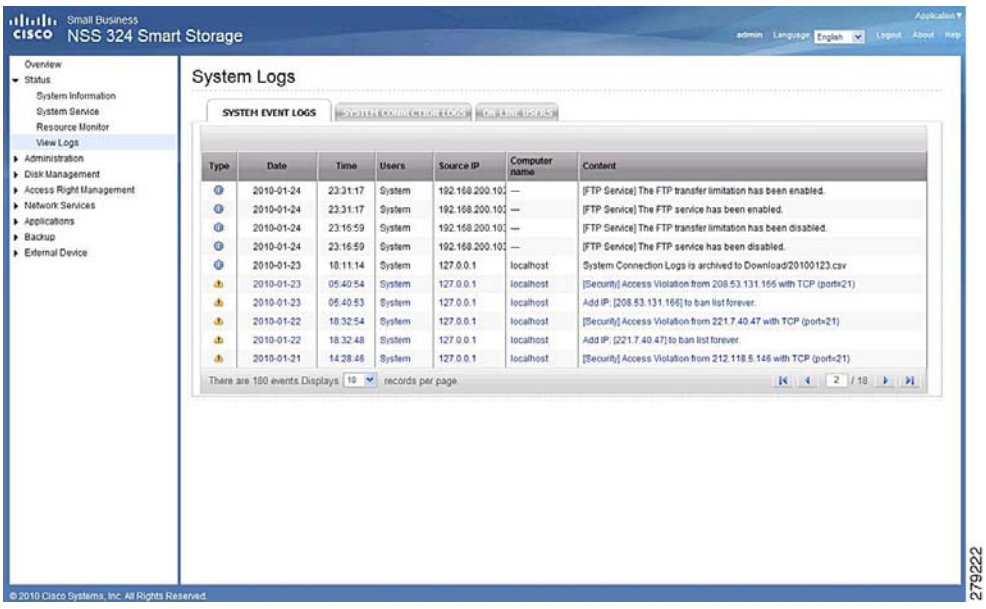
5. Enable System Connection Logs—Periodically checking the logs will help determine unauthorized users and the IP addresses of violators.

Figure 6 Cisco Smart Storage Logs of Violator's Addresses



6. Enable Network Access Protection—This automatically blocks the IP address of the violator and can be customized (block for a fixed duration or ban for life).

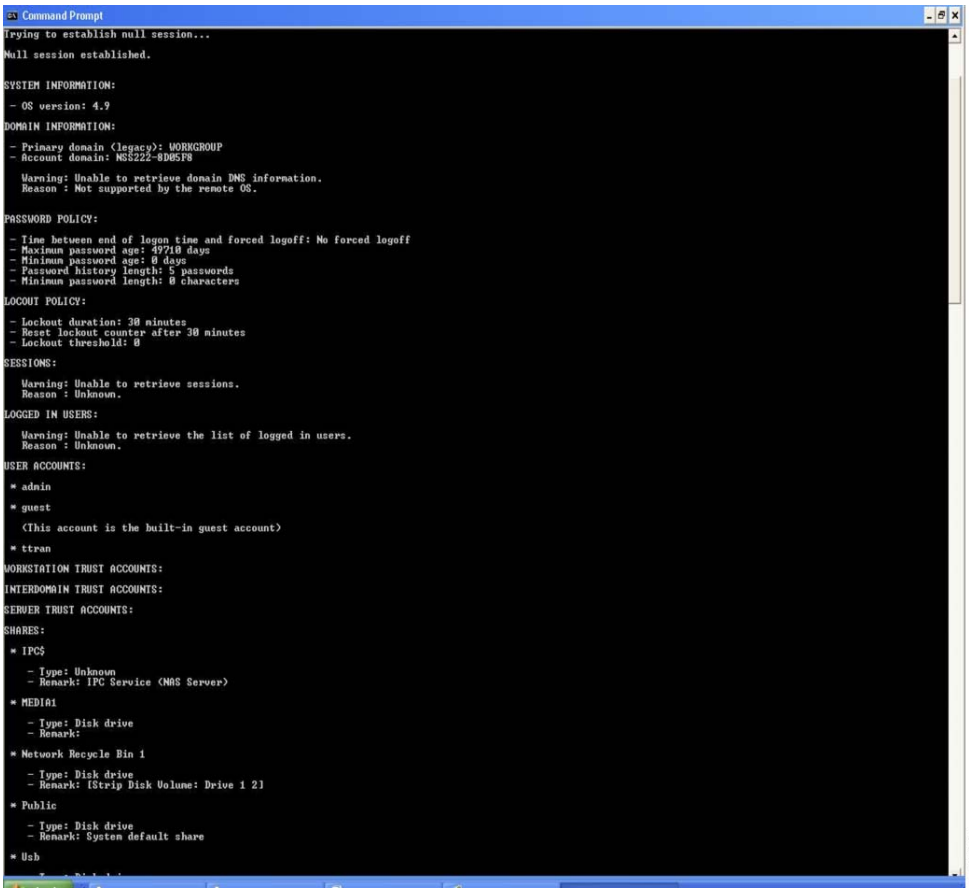
Figure 7 Cisco Smart Storage Built-in Network Access Protection (Violator's IP Address is Blocked From Accessing the System)



7. If possible use SNMPv3 instead of SNMPv2—SNMPv3 is more secure because it uses stronger Digest algorithms such as MD5 and SHA for authentication and encryption.

8. Disable Guest Account in all default shares (Public, Multimedia, etc.)—This helps to prevent Elevation of Privileges attack. Figure 8 shows the example of using guest (null session) to determine the NAS system information (i.e. user accounts, shares, password policy information, etc.)

Figure 8 Usage of Guest Account to Retrieve the System Information



9. Use HTTPS and disable HTTP—HTTPS is more secure and offers stronger encryption and authentication methods. HTTPS refers to the administrator UI.

10. Use a router with port forwarding to allow access to a specific TCP/UDP port. Disable all other TCP/UDP ports (this provides an additional level of protection). VPN is more secure than using port forwarding and should be used if available.

Figure 9 Example of Port Forwarding On the Cisco Small Business Router

11. If WiFi is enabled in your network, ensure that the wireless network is secured with WPA2 with AES.

12. By default, all the external USB and eSata disks have “Local Group=everyone” assigned as “Read only.” If your USB or eSata contains sensitive information then consider removing the “Local Group=everyone” on these shares.

13. Monitor the system log regularly for Access Violation and take action if necessary. Block the IP address from accessing the system via IP Filtering.

14. Utilize white list and black list types of Security Level Access Control. White list is preferable because it is safer to only allow certain IP addresses, rather than allowing every IP address except those on the back list.

Figure 10 Example of White List Access Control

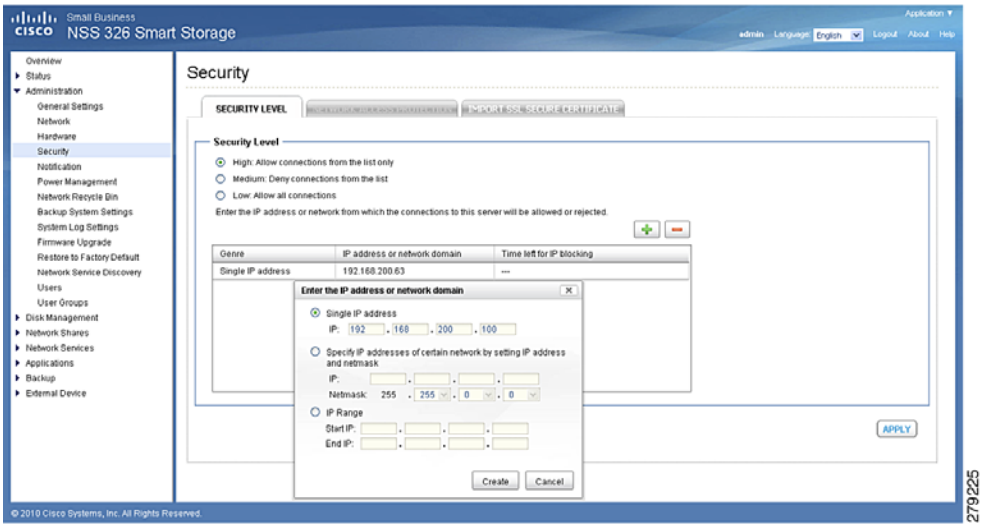
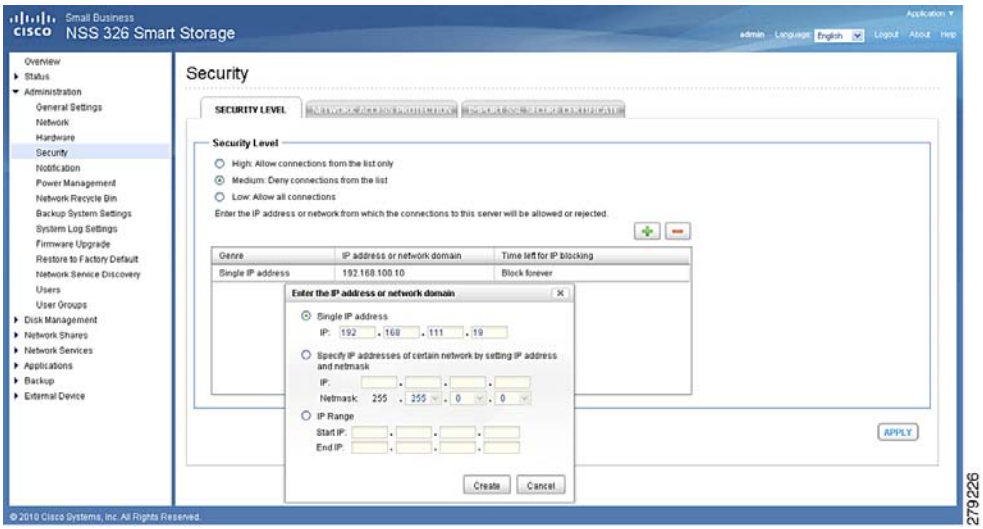


Figure 11 Example of Black List Access Control



Deployment Model Specific Security Considerations

Depending on the method of deployment, the security considerations for the NAS fall into one of these categories:

- Security considerations when the NAS is connected directly to the public Internet (Figure 1).
- Security considerations for the NAS with LAN only access (Figure 2).
- Security considerations when the NAS is accessible from the Internet via port forwarding on the router (Figure 3).
- Security considerations when running services on the NAS (web server, MySQL server, etc.)

Security Considerations When the NAS is Connected Directly to the Public Internet

This is the case where the user wants to have easy access to the files on the NAS from anywhere that has Internet access. Figure 1 shows this type of deployment. The access methods are either by FTP, SMB/CIFS or Web File Manager. In this configuration, the NAS is open to the public and most vulnerable to DoS and security hacks. To minimize these threats, please consider the following:

- Use and enforce complex passwords for admin and user accounts.
- Disable telnet and SSH.

- Enable FTPS instead of FTP. Also, verify that Anonymous FTP is not enabled
- Disable guest access on Network Share > Public.
- Enable Web File Manager and access the files on the NAS through a HTTPS connection.
- Enable Connection Log and Network Access Protection.
- Monitor the connection log regularly.
- Disable all Network Services and Applications that are not absolutely essential. In particular, the MySQL Server and Web Server applications should only be enabled if absolutely necessary in this configuration.
- Recommend limiting the exposure of the NAS in a DMZ to an environment using a dedicated router/firewall to minimize potential service disruption to the NAS device.

Security Considerations for the NAS with LAN Only Access

This is the most common and secure way for small businesses and households to deploy the NAS. Figure 2 shows this type of deployment. In this configuration, the NAS can be used as a file server or Media server. It is well shielded from the public Internet threats. In this configuration, consider employing the following:

- Use and enforce complex passwords for admin and user accounts.
- Verify that the LAN is not connected to the wireless gateway. If it is WiFi accessible, ensure that the wireless network is secured with WPA2 with AES.
- Enable Connection Log and Network Access Protection.
- Trojan horses, worms, and viruses are other forms of security threats. In any environment, it is very important to have adequate anti-virus protection software.

Security Considerations When the NAS Is Accessible From the Public Internet Via Port Forwarding On the Router

In this configuration, the NAS is deployed in a private LAN environment and can be accessed securely from the public Internet. Since it is exposed to the public Internet, the NAS is vulnerable if it is not properly configured. To minimize these security vulnerabilities, the following considerations are recommended:

- If VPN access will meet your needs, use that instead because it is more secure.

- Use and enforce complex passwords for admin and user accounts.
- If supported, enable DoS protection on the router.
- Define Access Control List (ACL) on the router or the NAS. The user can either define a list of allowable IP addresses (white list) or a list of prohibited IP addresses (black list). This way, access to the NAS is controlled.
- Enable only FTPS (Disable FTP and anonymous FTP) for remote file access.
- For remote management of the NAS, enable HTTPS and disable HTTP.
- Monitor the access log on the router and the NAS regularly for unauthorized accesses.

Security Considerations When Additional Services Are Running On the NAS (Web Server, MySQL, Media Server, etc.)

The NAS has a capability of hosting a web server and other services such as MySQL, media servers (iTunes Service, Multimedia Station, UPnP Media server). Because of this, the NAS introduces some unique security considerations that must also be addressed:

- Use and enforce complex passwords for admin and user accounts.
- Use a separate NAS for hosting the web server and/or Media Server. This way, if the security of the web server is compromised, the critical data is protected.
- Backup your web server data on a regular basis. This way, if something happens to the web server, it can always be restored.

  NOTE The Cisco Smart Storage offers secure remote replication for backing up data from one Smart Storage to another Smart Storage system.
- If your server uses MySQL to keep track of transactions, consider the following:
  - Change the default password for root account from “admin” and enforce the complex password rule on the new password.
  - Enforce the complex password on all user accounts.
  - Assign appropriate database access privilege levels (insert, add, drop, view, create, execute, etc.) to individual users.
  - Create a Client Access Control List for admin/root account. For example, only known list of IP addresses can access the database as root.

- Use HTTPS, when accessing phpMyAdmin for MySQL configurations.

  NOTE The Cisco Smart Storage enables HTTPS for phpMyAdmin access by default.

- Enable Access Control and monitor the access log regularly.

Cisco Smart Storage Security Configurations

Enable Password Strength Enforcement

To enable password strength enforcement:

STEP 1 Log in to the NAS by opening a web browser and entering the IP address of the NAS device. It is important to include the port 8080 following the IP address.

For example:

http://<NAS IP address>:8080

STEP 2 Choose **Administrator > General Settings** from the Navigation menu. The *General Settings* window opens.

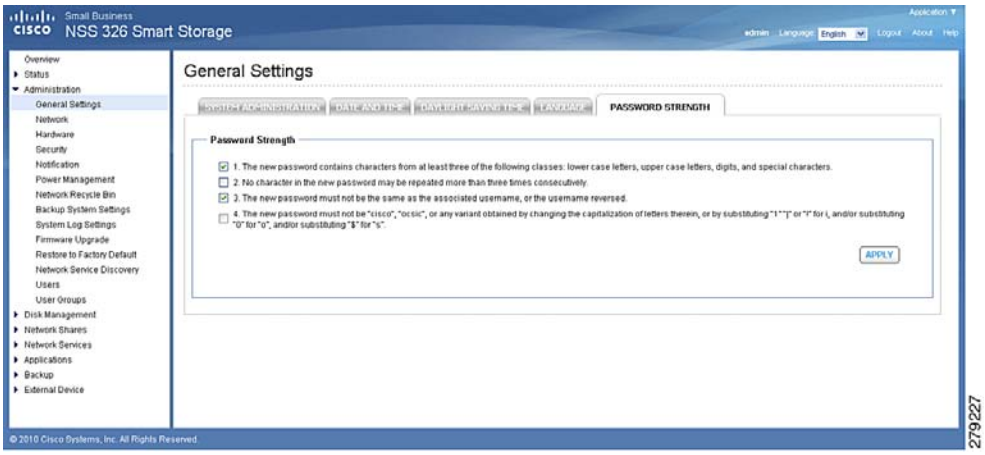
STEP 3 Select the **PASSWORD STRENGTH** tab.

STEP 4 Check the appropriate password enforcement. Cisco offers the flexibility of four levels of password strength enforcements.

STEP 5 Click **Apply**.

NOTE This should be done when the system is first configured. Please remember that the password strength enforcements are enforced for all new users and not on previously configured users.

Figure 12 Password Enforcement Configuration



Disable Telnet and/or SSH

To disable Telnet or SSH:

STEP 1 Log in to the NAS by opening a web browser and entering the IP address of the NAS device. It is important to include the port 8080 following the IP address.

For example:

http://<NAS IP address>:8080

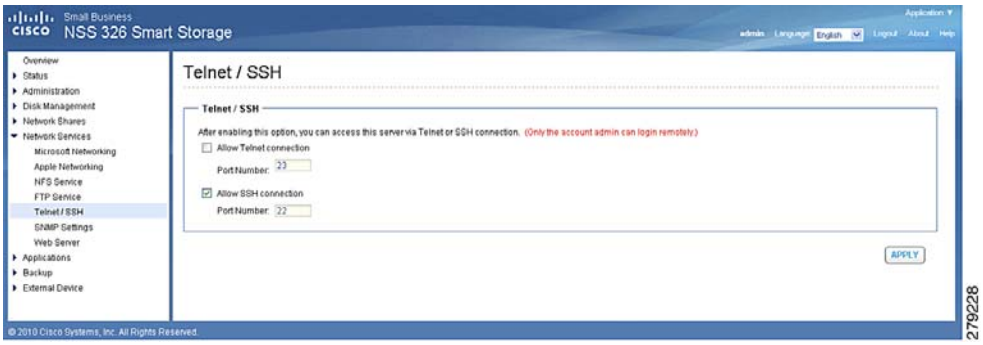
STEP 2 Choose **Network Services > Telnet/SSH** from the Navigation menu. The *Telnet/SSH* window opens.

STEP 3 Uncheck the **Allow Telnet** check box. This is unchecked by default

STEP 4 Uncheck the **Allow SSH** check box.

STEP 5 Click **Apply**.

Figure 13 Disable Telnet/SSH



Enable FTPS (Anonymous FTP Is Disabled By Default)

To enable FTPS:

STEP 1 Log in to the NAS by opening a web browser and entering the IP address of the NAS device. It is important to include the port 8080 following the IP address.

For example:

http://<NAS IP address>:8080

STEP 2 Choose **Network Services > FTP Service** from the Navigation menu. The *FTP Service* window opens.

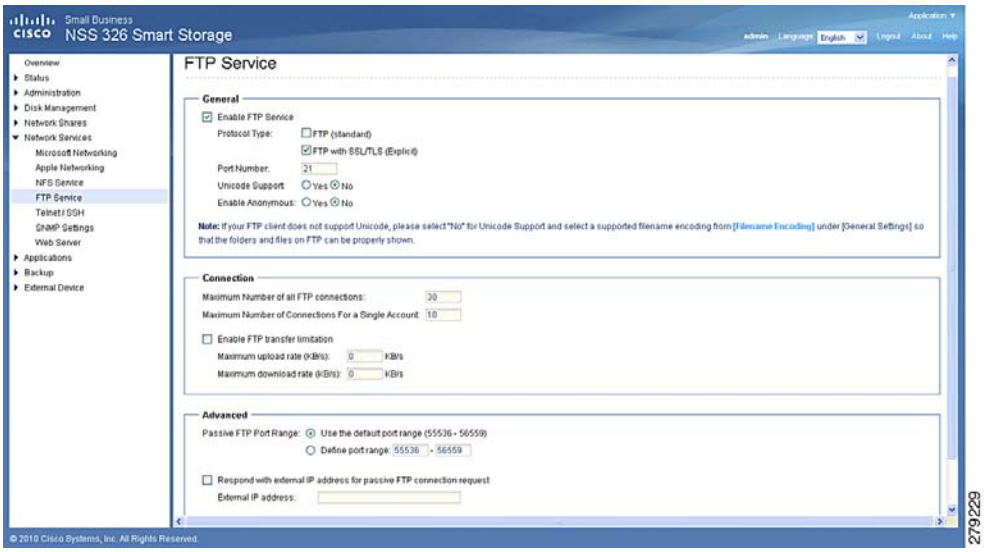
STEP 3 Uncheck the **FTP Standard** check box and check **FTP with SSL**.

STEP 4 Use the default values for all other parameters.

STEP 5 Click **Apply**.

NOTE To access the system that is configured only for FTPS, the user also needs to set the FTP client to FTPS (explicit).

Figure 14 FTP Configuration



Enable System Connection Logs

To enable system connection logs:

STEP 1 Log in to the NAS by opening a web browser and entering the IP address of the NAS device. It is important to include the port 8080 following the IP address.

For example:

http://<NAS IP address>:8080

STEP 2 Choose **Administration > System Log Settings** from the Navigation menu. The *System Logs* window opens.

STEP 3 Select the **SYSTEM CONNECTION LOGS** tab.

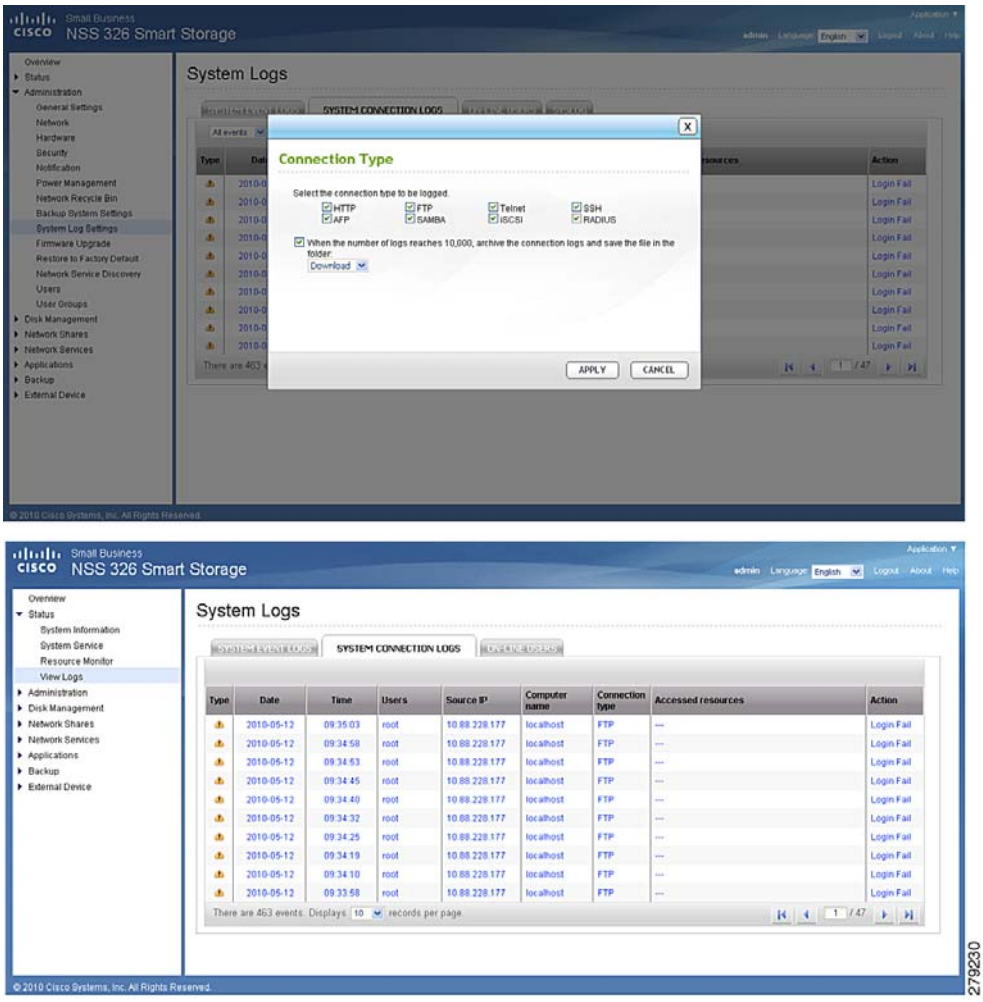
STEP 4 Click **Options** and check all connection types to be logged (HTTP, FTP, Telnet, SSH, AFP, SAMBA, iSCSI).

STEP 5 Check and select the Network Share to save the log file. The default share is Download.

STEP 6 Click **APPLY**.

STEP 7 Click **Start Logging** to start the log process.

Figure 15 Connection Login Configuration



Enable Network Access Protection

To enable network access protection:

STEP 1 Log in to the NAS by opening a web browser and entering the IP address of the NAS device. It is important to include the port 8080 following the IP address.

For example:

http://<NAS IP address>:8080

STEP 2 Choose **Administration > Security** from the Navigation menu. The *Security* window opens.

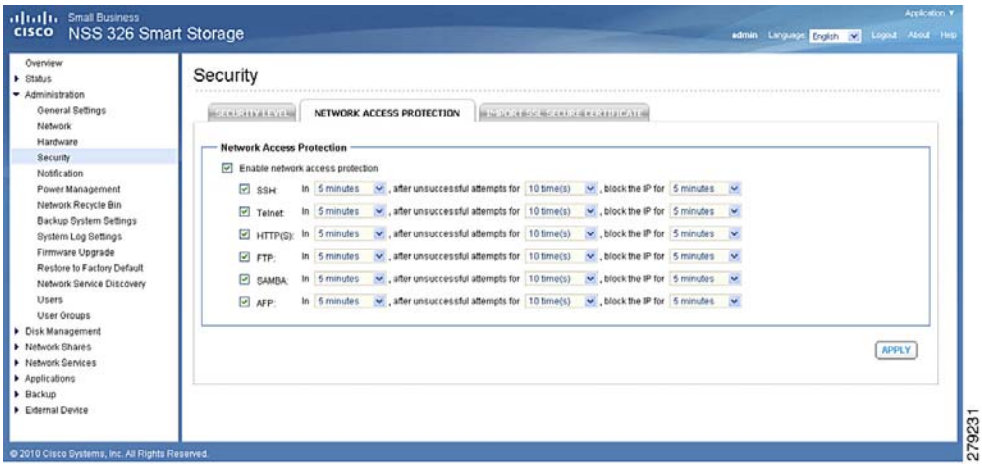
STEP 3 Select the **NETWORK ACCESS PROTECTION** tab.

STEP 4 Check the **Enable Access Protection** check box.

STEP 5 Check the desired Network Protocols and select the desired access protection parameters. For example, allowable unsuccessful attempts and blocked duration (5 minutes, 30 minutes, 1 hour, 1 day, or forever).

STEP 6 Click **APPLY**.

Figure 16 Network Access Protection Configuration



Enable SNMPv3

To enable SNMPv3:

STEP 1 Log in to the NAS by opening a web browser and entering the IP address of the NAS device. It is important to include the port 8080 following the IP address.

For example:

http://<NAS IP address>:8080

STEP 2 Choose **Network Services > SNMP Settings** from the Navigation menu. The *SNMP Settings* window opens.

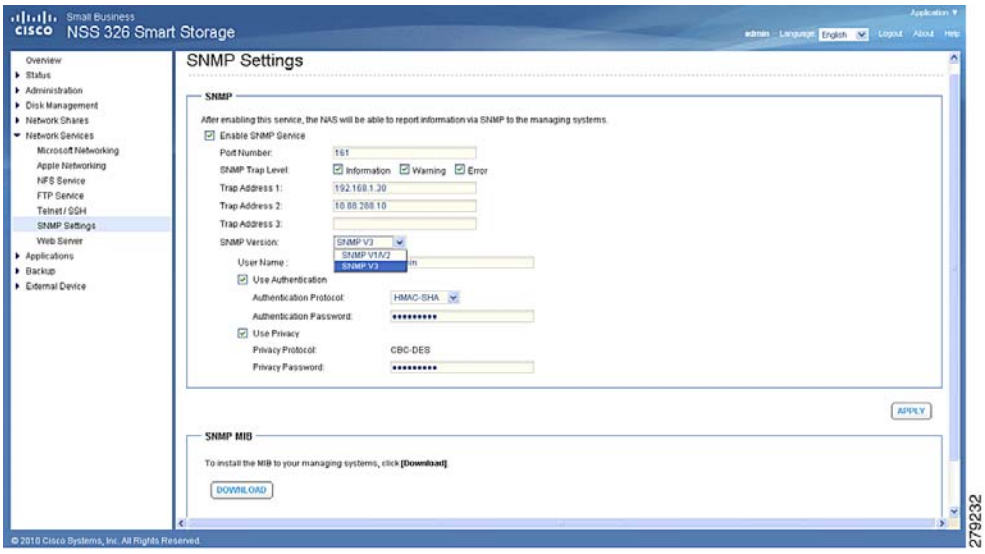
STEP 3 Check the **Enable SNMP Service** check box and select the SNMP Version to be **SNMPv3**.

STEP 4 If the "Use Authentication" method is used, check this box and enter the Authentication Protocol (**HMAC-MD5** or **HMAC-SHA**).

STEP 5 If the "Use Privacy" Method is used, check this box and enter the Privacy Password.

STEP 6 Click **Apply**.

Figure 17 SNMP Configuration



Disable Guest Access on Network Default Shares

To disable guest access on the network default shares:

STEP 1 Log in to the NAS by opening a web browser and entering the IP address of the NAS device. It is important to include the port 8080 following the IP address.

For example:

http://<NAS IP address>:8080

STEP 2 Choose **Administration > Network Share > Share Folders** from the Navigation menu. The *Share Folders* window opens.

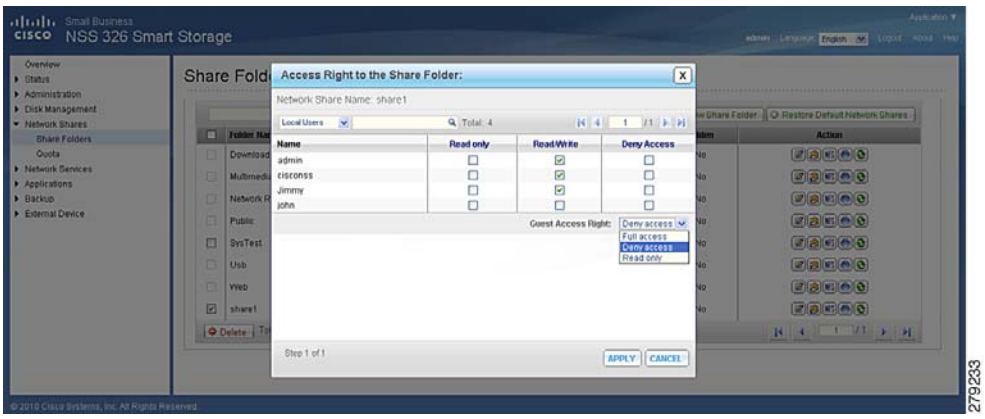
STEP 3 For each of the Default Network Shares (Multimedia, Public, etc.) do the following:

a. Click on Access Control (the hands shake icon under the Action tab).

b. Select **Deny Access** for Guest Access Right.

c. Click **APPLY**.

Figure 18 Access Right Configuration



Use HTTPS and disable HTTP

To disable HTTP and use HTTPS:

STEP 1 Log in to the NAS by opening a web browser and entering the IP address of the NAS device. It is important to include the port 8080 following the IP address.

For example:

http://<NAS IP address>:8080

STEP 2 Choose **Administration > General Settings** from the Navigation menu. The *General Settings* window opens.

STEP 3 Select the **SYSTEM ADMINISTRATION** tab.

STEP 4 Check the **Force secure connection (SSL) only** check box.

STEP 5 Click **APPY**.

NOTE After enabling the "Force secure connection (SSL) only" option, the web Administration can only be connected via HTTPS.

Figure 19 HTTP/HTTPS Configuration

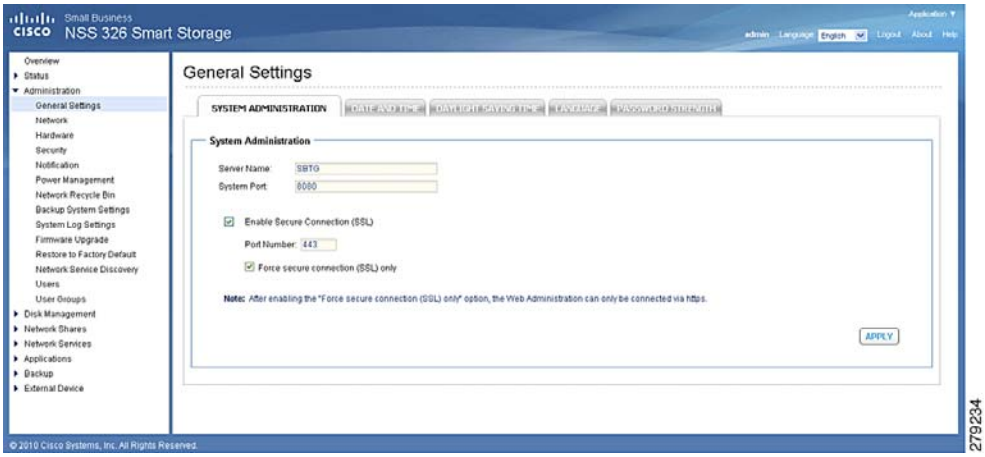
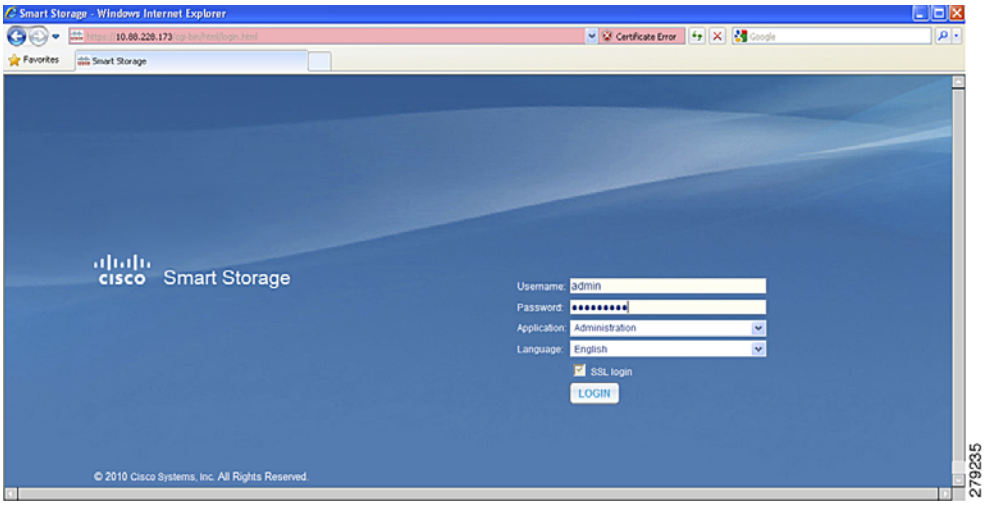


Figure 20 Example of HTTPS Access



Security Level Configuration

To configure the security level:

STEP 1 Log in to the NAS by opening a web browser and entering the IP address of the NAS device. It is important to include the port 8080 following the IP address.

For example:

http://<NAS IP address>:8080

STEP 2 Choose **Administration > Security** from the Navigation menu. The *Security* window opens.

STEP 3 Select **High** if you want to implement a white list type of access.

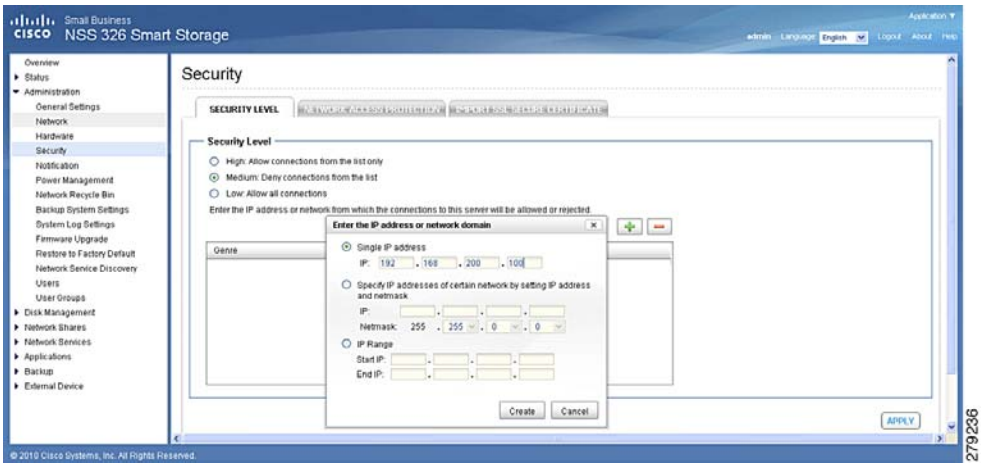
STEP 4 Select **Medium** if you want to implement a black list type of access.

STEP 5 Click + and enter the IP Address to the list.

STEP 6 Click **Create**.

STEP 7 Click **APPLY**.

Figure 21 Security Level Configuration



Conclusion

"You can't outrun the Bear" but there are ways to avoid being eaten. One is to be faster than the guy next to you. The other is to make it difficult and not worth the effort for the bear to chase you. In either case, you have to do something. It is difficult to render the system bullet-proof from hackers and attacks without effecting the system usability and accessibility. The key is to consider the trade-offs very carefully between the convenience and utility of enabling WAN based access to the NAS, and various services (MySQL, Web Server, etc.) versus the security risks. If improperly assessed, the end result can lead to loss of sensitive information (confidential company information, marketing strategies, etc.), correspondence (emails, contacts), or financial details.

OL-23025-01