How To Configure SSL Authentication on an IP Appliance from Clish and Voyager

6 May 2012
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=16581
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/6/2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How To Configure SSL Authentication on an IP Appliance from Clish and Voyager ).
How To Configure SSL Authentication on an IP Appliance from Clish and Voyager

Objective

This document explains how to configure SSL Authentication for Voyager web access from Voyager or the Clish command line.

Supported Versions

Any

Supported Operating Systems

Any IPSO

Supported Appliances

Any IP appliance

Supported Encryption

None (Disable SSL)
40-bit key or stronger
56-bit key or stronger
128-bit key or stronger
Require Triple-DES

Before You Start

Related Documents and Assumed Knowledge

- How to view Voyager's SSL certificate expiry date from command line? - sk41090 (http://supportcontent.checkpoint.com/solutions?id=41090)
- Connecting to Voyager SSL Access shows "The page cannot be displayed" - sk39357 (http://supportcontent.checkpoint.com/solutions?id=39357)
- How to create SSL key from clish in Voyager - sk53329 (http://supportcontent.checkpoint.com/solutions?id=53329)
Impact on Environment and Warnings

If you use SSL Network Extender and you enable HTTPS in Voyager, complications occur. SSL Network Extender fails. You need to change the port number for HTTPS in Voyager.

Overview

To configure SSL Authentication in Voyager, you need to configure Voyager to use HTTPS. HTTPS (Hypertext Transfer Protocol Secure) authentication provides an additional layer of security when you connect to Voyager. SSL provides secure channel for sensitive data on a network. This ensures protection of valuable data from eavesdroppers. HTTPS in Voyager uses server certificates that are generated within Voyager or Clish.

Introduction and FAQ:

- **What is HTTPS?**
  HTTPS (Hypertext Transfer Protocol) Secure is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communication and secure identification of a network web server.

- **What is SSL/TLS?**
  Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security for communications over networks such as the Internet.

- **What port does HTTPS use?**
  By default HTTPS uses port 443. This can be changed within Voyager or Clish.

Configuring SSL Authentication on an IP Appliance from Voyager

1. Log into Voyager with HTTP. You can launch Voyager from any Web based browser and use the IP address or DNS name of the firewall. For example, http://172.26.143.105. Use your login details to authenticate for Voyager.
2. In the Voyager tree view, select **Configuration > Security and Access > Voyager Web Access > Install Certificate for SSL**. The Install Certificate for SSL window opens.

![Voyager tree view with selected Install Certificate for SSL](image)


![Generate Certificate for SSL (Request) window](image)

4. To configure the Generate Certificate for SSL (Request) window:
   - In **What to Generate**, select **A Self-signed X.509 certificate**.
   - In **Private Key Size**, select **512** or **768** or **1024**.
Configuring SSL Authentication on an IP Appliance from Voyager

Specifies how large your newly generated private key is in bits. Larger sizes are generally considered more secure. The default is 1024.

In the Set Passphrase field, enter a string for this tool to use to encrypt your new private key. If you do not wish to use a passphrase, enter: ""

In the Verify Passphrase field, enter your chosen passphrase again.

In the Country Name field, enter a two letter code that indicates your country. For example, US. This is a required entry.

In the State or Province Name field, enter the name of your state or province. This is a required entry.

In the Locality (Town) Name field, enter the name of your city or town. For example, Sunnyvale. If you do not wish to use a passphrase, enter: ""

In the Organization Name field, enter the name of your company or organization. For example: Worldwide Widgets. This is a required entry.

In the Organizational Unit Name field, enter the name of a subunit within your company or organization. If you do not wish to use a passphrase, enter: ""

In the Common Name (FQDN) field, enter a name that identifies where the certificate goes. The name is most commonly the fully qualified domain name for your platform. For example, www.ship.wwidgets.com. If you generate a request for a certificate authority, the issuer may impose a different standard.

In the Email Address field, enter an e-mail address that can be used to contact the person responsible for the platform and its certificate. For example, webmaster@ship.wwidgets.dom.

5. Click Apply. The New x.509 Certificate and New Private Key window opens.
6. Copy each key output to a text editor for a reference.

7. Click the Voyager SSL certificate page. The Install Certificate for SSL window opens.

   Your certificate's MD5 fingerprint is: 31:84:34:7C:F0:89:84:9C:0A:2D:4E
   Your certificate's SHA-1 fingerprint is: 2A:7E:2E:7E:91:CA:4B:1D:3B:8D:3D:70:1B

   To install your new certificate, copy it and your private key into the Voyager SSL certificate page.

   When copying certificates, certificate requests, and keys, remember to include the dashed lines.

8. Copy and paste the output kept on a text editor from the previous window to the respective fields. Also, enter your own private key.

   **Note** - Make sure there is no space at the end of each key. If you leave a space, you get an error message and the certificate is not installed.
9. Click Apply. The window is refreshed, and reads Apply Successful.

10. From the Voyager tree view, select Voyager Web Options. The Voyager Web Options Configuration window opens.

11. In Require Encryption, select the Encryption key you want to use. The default is None.
12. Click **Apply** and **Save**. You are logged out of Voyager and you need to log in with HTTPS.

---

**Configuring SSL Authentication on an IP Appliance from Clish**

1. Open an SSH Access or a Console Access to the IPSO Firewall.
2. From the IPSO command line, run: `clish`
3. To better ensure your security, you should generate the certificate and private key over a trusted connection. To generate a certificate and its associated private key run:

   ```
   NokiaIP260:106> generate voyager ssl-certificate key-bits <512 | 768 | 1024> <passphrase name | prompt-passphrase> country name state-or-province name locality name organization name organizational-unit name common-name name email-address name <cert-file path | cert-request-file path> key-file path
   ```

   **Where:**
   - For **key bits**, enter 512 or 768 or 1024.
   - Specifies how large your newly generated private key is in bits. Larger sizes are generally considered more secure. The default is 1024.
   - `<passphrase name | prompt-passphrase>` is a string for this tool to use to encrypt your new private key (repeat the string to verify). If you do not wish to use a passphrase, enter: ""
   - **country name** is a two letter code that indicates your country. For example, US. This is a required entry.
   - **state-or-province name** is the name of your state or province. This is a required entry.
   - **locality name** is the name of your city or town. For example, Sunnyvale. If you do not wish to use a passphrase, enter: ""
   - **organization name** is the name of your company or organization. For example: Worldwide Widgets. This is a required entry.
   - **organizational-unit name** is the name of a subunit within your company or organization. If you do not wish to use a passphrase, enter: ""
   - **common-name name** is a name that identifies where the certificate goes. The name is most commonly the fully qualified domain name for your platform. For example, www.ship.wwwidgets.com. If you generate a request for a certificate authority, the issuer may impose a different standard.
   - **email-address name** is an e-mail address that can be used to contact the person responsible for the platform and its certificate. For example, webmaster@ship.wwwidgets.com.
   - **cert-file path** is the file that receives a certificate. The keyword should be followed by the path name to a file on the IPSO system. Use absolute pathnames. The certificate is signed with an SHA-1 hash.
How To Configure SSL Authentication on an IP Appliance from Clish and Voyager

4. To install a certificate and private key, run these commands to copy a certificate and its associated private key in the /var/etc/voyager_ssl_server.crt and /var/etc/voyager_ssl_server.key files.

```
NokiaIP260:106> set voyager ssl-certificate cert-file path
key-file path <passphrase name | prompt-passphrase> web connections.
```

Where:
- `cert-file path` is a file that contains the certificate you want to copy. The keyword should be followed by the path name to the file on the IPSO system. Use absolute pathnames.
- `key-file path` is a file that contains the private key you want to copy. The keyword should be followed by the path name to a file on the IPSO system. Use absolute pathnames.
- `passphrase name` is the passphrase used by you to generate the certificate and private key or certificate request.
- `prompt-passphrase` is to repeat the passphrase.

5. To set the Voyager web access to your desired Encryption key setting, run:

```
NokiaIP260:106> set voyager ssl-level <value>
```

Where:
- `<value>` is the required level of security for Voyager web connections. The value zero (0) indicates that SSL-secured connections are not used. To set the level of encryption, remote connections are required to use a level of encryption at least as strong as the one you specify. These are the standard encryption levels:
  - 40-bit
  - 56-bit
  - 128-bit
  - 168-bit (Triple-DES)

6. To access your platform, change your URL from: `http://hostname/` to: `https://hostname/`

7. To save the configuration, run: `save config`

8. To execute and save the changes, run: `NokiaIP260:106> save config`

   You can log into Voyager with HTTPS.

To reset Voyager back to HTTP from the command line (if you wish):

Run: `voyager -e 0 80`