

finjan[®]
Vital Security™

securing your web

NG-8000



NG-6000



NG-5000

Integrated SSL Scanning

Software Version 9.0

Copyright

© Copyright 1996-2008. Finjan Software Inc. and its affiliates and subsidiaries ("Finjan").

All rights reserved.

All text and figures included in this publication are the exclusive property of Finjan and are for your personal and non-commercial use. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, use or sell any part of its content in any way without the express permission in writing from Finjan. Information in this document is subject to change without notice and does not present a commitment or representation on the part of Finjan.

The Finjan technology and/or products and/or software described and/or referenced to in this material are protected by registered and/or pending patents including U.S. Patents No. 3952315, 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968, 7058822, 7076469, 7155743, 7155744 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dote and Window-of-Vulnerability are trademarks or registered trademarks of Finjan. Sophos is a registered trademark of Sophos plc. McAfee is a registered trademark of McAfee Inc. Kaspersky is a registered trademark of Kaspersky Lab. Websense® is a registered trademark of Websense, Inc. IBM® Proventia® Web Filter is a registered trademark of IBM Corporation. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation. All other trademarks are the trademarks of their respective owners.

For additional information, please visit www.finjan.com or contact one of our regional offices:

<p>USA: San Jose 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com</p>	<p>Europe: UK 4th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com</p>
<p>Europe: Netherlands Printerweg 56 3821 AD Amersfoort, Netherlands Tel: +31 334 543 555 Fax: +31 334 543 550 salesne@finjan.com</p>	<p>Europe: Germany Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com</p>
<p>Israel/Asia Pacific Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com</p>	

Catalog name: ISC-FD-9.0-02

Email: support@finjan.com

Internet: www.finjan.com

Table of Contents

1. Introduction	1
2. HTTPS Scanning	1
2.1 On the Fly Certificate Generation	1
2.2 Certificate Validation	2
2.3 SSL Certificate Errors	6
3. HTTPS Policies	11
4. Configuring HTTPS Support	11
4.1 HTTPS Configurable Parameters	12
5. Transparent HTTPS	14

1. Introduction

The main role of Secure Socket Layer (SSL) is to provide security for Web traffic. Security includes confidentiality, message integrity, and authentication. SSL achieves these elements of security through the use of cryptography, digital signatures, and certificates.

The Finjan Vital Security series is an enterprise solution which protects users and organizations from Web attacks, including attacks traveling inside encrypted HTTPS communication. The HTTPS functionality is integrated into the Vital Security NG appliance, providing unified setup, management, authentication and identification as well as the ability for system administrators to set HTTPS policies.

The HTTPS scanning solution protects enterprise networks by decrypting HTTPS traffic and inspecting it for viruses, worms and malicious code and by providing encrypted Web attack protection, certificate validation and content filtering.

Integrated HTTPS scanning is a license based feature which enables the scanning server to be configured to support HTTPS. HTTPS configuration can be carried out system wide or per Scanning Server.

In addition to the scanning solution for HTTP traffic, Finjan also provides certificate validation functionality. This ensures that corporate policies regarding certificates are enforced by automatically validating each certificate and ensuring that the chain goes back to the trusted authority. In this way, corporate policies are maintained while users are provided with the benefit of being able to access SSL traffic.

2. HTTPS Scanning

When HTTPS scanning is enabled, the Vital Security Scanning Server acts as a “man in the middle” meaning that the end-user requests the server’s certificate from the Scanning Server, which fetches it from the original web server. The Scanning Server then validates the certificate and according to the security policy, sends it to the user or blocks it. This transaction includes two sessions: one session between the client and the Scanning Server and another session between the Scanning Server and the original web server.

2.1 On the Fly Certificate Generation

When HTTPS Scanning is enabled, there are two HTTPS connections for each session: a connection between the end-user and the Scanning Server and a connection between the Scanning Server and the HTTPS server. When the end-user first sends the request to the Scanning Server, the Scanning server does not have the certificate of the original web server, so it has to fetch the certificate before establishing the connection. The Scanning Server fetches the certificate from the HTTPS server and

then it generates, on the fly, a new certificate, which includes the same information as the original certificate. The Scanning Server signs the new certificate with its own private key and sends it to the end-user.

2.2 Certificate Validation

Vital Security HTTPS ensures that corporate policies for certificates are enforced, while removing the decision from the end-user's hands by automatically validating each certificate and making sure that the chain goes back to the trusted authority. Policies regarding certificates are enforced by checking individual certificate names, expiry dates, trusted authority chains and revocation lists.

A list of trusted certificate authorities is supplied with the system and used for digital signature analysis and for HTTPS certificate validation. Digital certificate lists are updated via Finjan security updates. These lists include the required trusted certificate authorities as well as the Certificate Revocation Lists (CRLs).

Certificate validation is based on the action taken for policy type (Bypass / Inspect Content / User Approval). When Bypass is selected, the original server certificate is obtained and certificate validation is not performed by the system (i.e. no security or https validation carried out on traffic). If Inspect Content or User Approval is selected, the server certificates are analyzed and replaced by a certificate containing the same mismatches as the original one. The resulting mismatches are compared against SSL certificate conditions.

To view the certificate validation rules navigate in the Management Console to Policies → Condition Settings → HTTPS Certificate Validation → Default Certificate Validation Profile.

You can also duplicate the default profile and adjust it to your organization's needs.

The Default Certificate Validation Profile comprises the certificate error events.

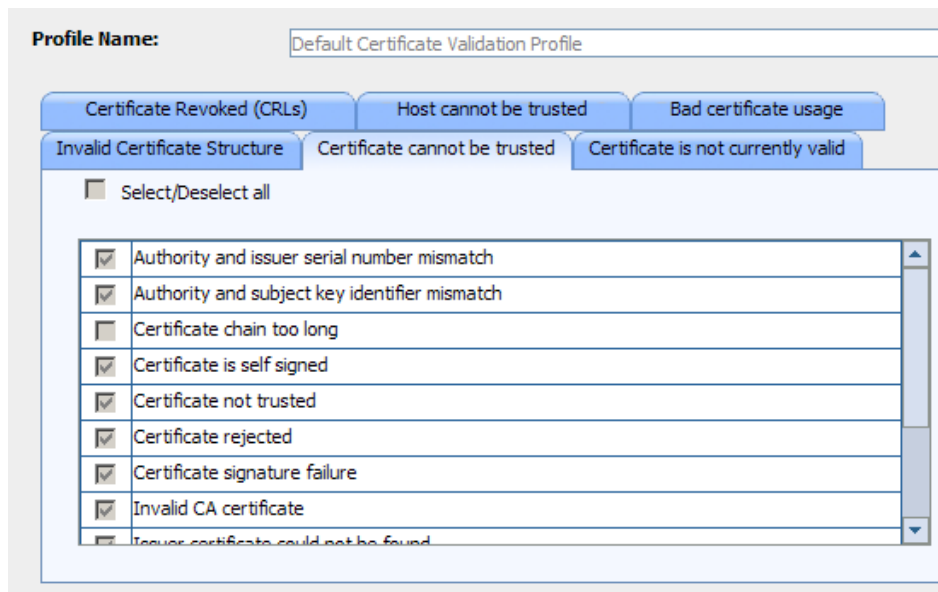


Figure 1: Certificate Validation Profile

The table below describes each option in the HTTPS certificate validation profile:

2.2.1 Certificate Revoked (CRLs)

Field	Description
Unable to get certificate CRL	The CRL of a certificate could not be found.
Unable to decrypt CRL's signature	This means that the actual signature value could not be determined rather than it not matching the expected value.
CRL signature failure	The signature of the certificate is invalid.
Certificate is not yet valid	The notBefore date is after the current time.
Certificate has expired	The notAfter date is before the current time.
Format error in CRL's lastUpdate field	The CRL lastUpdate field contains an invalid time.
Format error in CRL's nextUpdate field	The CRL nextUpdate field contains an invalid time.
Certificate revoked	The certificate has been revoked.

2.2.2 Host cannot be Trusted

Field	Description
Hostname does not match Certificate name	The host name mismatches the one mentioned in the certificate.
Cannot verify Hostname	The host name is unavailable and therefore cannot be verified against the certificate.

2.2.3 Bad Certificate Usage

Field	Description
Unsupported certificate purpose	The supplied certificate cannot be used for the specified purpose.
Path length constraint exceeded	The basic Constraints path length parameter has been exceeded.

2.2.4 Invalid Security Structure

Field	Description
Certificate signature cannot be decrypted	The certificate signature could not be decrypted (meaningful for RSA keys).
Cannot decode issuer public key	The public key in the certificate SubjectPublicKeyInfo could not be read.

2.2.5 Certificate Cannot be Trusted

Field	Description
Issuer certificate could not be found	This occurs if the issuer certificate of an untrusted certificate cannot be found.
Certificate signature failure	The signature of the certificate is invalid.
Certificate is self signed	The certificate is self signed and the same certificate cannot be found in the list of trusted certificates.
Root certificate could not be found locally	The certificate chain could be built up using the untrusted certificates but the root could not be found locally.

Field	Description
Unable to get local issuer certificate	The issuer certificate of a locally looked up certificate could not be found. This normally means the list of trusted certificates is not complete.
Unable to verify the first certificate	No signatures could be verified because the chain contains only one certificate and it is not self signed.
Certificate chain too long	The certificate chain length is greater than the supplied maximum depth.
Invalid CA certificate	Either it is not a CA or its extensions are not consistent with the supplied purpose.
Certificate not trusted	The root CA is not marked as trusted for the specified purpose.
Certificate rejected	The root CA is marked to reject the specified purpose.
Subject issuer mismatch	The current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate.
Authority and subject key identifier mismatch	The current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate.
Authority and issuer serial number mismatch	The current candidate issuer certificate was rejected because its issuer name and serial number was present and did not match the authority key identifier of the current certificate.
Key usage does not include certificate signing	The current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing.

2.2.6 Certificate is not currently valid

Field	Description
Certificate is not yet valid	The notBefore date is after the current time.
Certificate has expired	The notAfter date is before the current time.

2.3 SSL Certificate Errors

When the end-user opens the HTTPS session, the Scanning Server has to encrypt and decrypt the data between the end-user and the Scanning Server. The Scanning Server uses the certificate it generated (as described above). As the certificate is self-signed by Finjan, and is not trusted by the end-user's browser, the user will get a warning message:

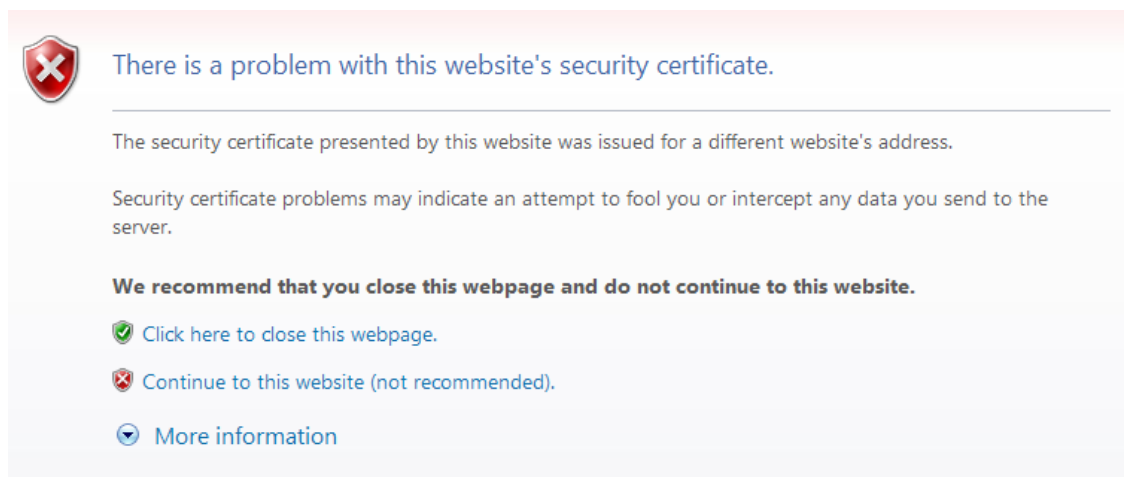


Figure 2: Internet Explorer Warning Message

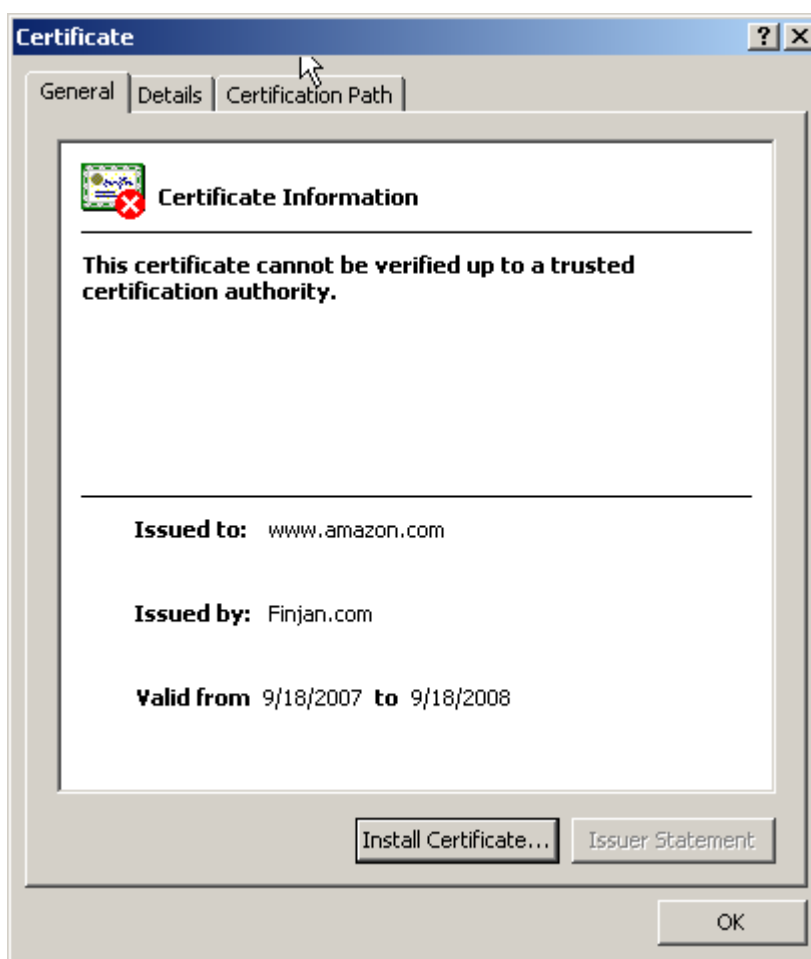


Figure 3: Certificate Details

In order to prevent the end-users from getting this warning message, system administrators can do one of the following:

- ◆ Install Finjan's certificate on the end-user's browser as a trusted root certificate authority.
- ◆ Install a certificate on all the Scanning Servers, issued by the organization's CA root certificate, which is already trusted by all users.



NOTE: Using a certificate from a trusted CA (such as VeriSign) will not prevent the certificate validation check, as it does not contain the remote HTTPS server's host name.

2.3.1 Installing Finjan certificate on the end-user's browser

The following procedures are relevant for Vital Security Software Versions 8.5.0, 8.5.0-M01 and 9.0:

⇒ To install Finjan's certificate as a trusted root CA:

1. Paste the certificate below into an empty file and save it as Finjan.cer

```
-----BEGIN CERTIFICATE-----
MIICtDCCAh2gAwIBAgIJAK7xcFlVJL+4MA0GCSqGSIb3DQEBBQUAMIGSMQswCQYD
VQQGEwJTTDEPMA0GA1UECBMU2hhcm9uMRAwDgYDVQQHEwdOZXRhbnlhMQ8wDQYD
VQQKEwZGaw5qYW4xZmZAVBgNVBAsTD1ZpdGFsIFNlY3VyaXR5MRMwEwYDVoDQDEwpG
aW5qYW4uY29tMSEwHwYJKoZIhvcNAQkBFhJzYWxlc21zQGZpbmphaW5jb20wHhcN
MDcwNTI1MTgxODI2WhcNMjcwNTI1MTgxODI2WjCBkjELMAkGA1UEBhMCSUwxDzAN
BgNVBAGTB1NoYXJvbWVjEQMA4GA1UEBxMHTmV0YW55YTEPMA0GA1UEChMGRmluamFu
MRcwFQYDVQQLLEw5WaxRhbCBTZWN1cm10eTETMBEGA1UEAxMKRmluamFuLmNvbTEh
MB8GCSqGSIb3DQEJARYSc2FsZXNpc0BmaW5qYW4uY29tMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQCarbcmg9MMkjFbOoknfmG0sWiyCiwtnIZ1vyP4cGRoC9Ly
8hwowO+kW9AjkGcCgCbssfFivqOSoxFFXwH7k3Cg3sU6vvjC8eMBZEYpeOEJ9dN
fsyqxrKG9ELr7q3POdu9lpFdYnE3BHxKDw0yRXdTfk1SBpyofWo4mdW6KrmTmwID
AQABoxAwDjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4GBAEo5s2ZCnPT0
i13PZ8vNdRIARbEv5mgXooyvE1Z3XyQVjbm6k6hQDdCgWw8+XxuBxY4NgSi6uI3
dIXmNxhaEozMNOcGKGLC363q05iYc5druMSd/cq8GmCM0cvJtsbCsigLBkIZNJk8
cbkxqCtOkha2KiCKy/JqpuLU0MuXs00Q
-----END CERTIFICATE-----
```

2. Install the certificate on the browser:

⇒ **To install the certificate on Internet Explorer:**

- In the control panel, click Internet Options.
- Click the Content tab and then the Certificate button.
- Click the Trusted Root Certification Authorities tab and then click the Import button.
- Click Next and then Browse. Navigate to the Finjan.cer file and click Open followed by Next, Next and Finish.



NOTE: For Microsoft based networks, it is possible to install the certificate for all the users at once using the Microsoft Group Policy Manager Console.

⇒ **To install the certificate on Firefox 3:**

- In Firefox, click Tools and Options
- Click Advanced and then the Encryption tab.
- Click the View Certificate button followed by the Authorities tab and then click Import.
- Navigate to the location of the Finjan.cer file and click Open.
- In the Downloading Certificate window, select "Trust this CA to identify web site" and click ok.
- Click OK twice to return to Firefox.

The following procedures are relevant for Vital Security Software Versions 8.5.0-M02, 9.0-M01 and onwards:

⇒ **To create a Self Signed Certificate:**

- Using an ssh client such as putty, connect to the Vital Security Limited Shell

2. Enter the command: `generate_ca_keys`
3. Choose the first option `1. Create a default self-signed certificate.`
A certificate is created.
4. Copy the certificate and send it to the end-users in your organization
5. In the Limited Shell, enter the command: `deploy_ca_keys`.

⇒ **To create and use a Certificate Signing Request:**

1. Using an ssh client such as putty, connect to the Vital Security Limited Shell
2. Enter the command: `generate_ca_keys`
3. Choose option `2. Create a certificate signing request (CSR) to be signed separately`
4. You will then be prompted to fill in all the details for the certificate authority.
5. After confirming the details, a certificate signing request is created. Copy this into a separate text file to send to a certificate authority.
6. Once you have a certificate back, send it to your end-users to install on their browsers.
7. In the Limited Shell, enter the command: `deploy_ca_keys`

⇒ **To add the certificate to your Internet browser (IE):**

1. Save the CER file to your desktop.
2. Double-click on the file.
The Certificate Information window appears.
3. Click on Install Certificate.
The Certificate Import Wizard opens.
4. Navigate through the wizard till the end. The Finjan certificate is now added to the browser's trusted sites list.
You can check it is there by navigating in your browser to Tools → Internet Options → Content → Certificates → Trusted Root Certification Authorities

⇒ **To add the certificate to your Internet browser (Firefox 3):**

1. Save the CER file to your desktop.
2. In Firefox, navigate to Tools → Options.
3. Click on the Advanced option (top right)
4. Click on the Encryption tab.
5. Click on View Certificates.

6. Click on the Authorities tab.
7. Click Import and browse to the CER file.
8. In the Downloading Certificate window, select “Trust this CA to identify web site” and click ok.
9. Click OK twice.

2.3.2 Installing Root Certificate on the Scanning Server

If the organization has trusted root CA, a root certificate can be generated and imported to the Scanning Server. In this case, the users are already configured to trust the organizations root CA and there is no need to configure anything for the users.

⇒ **To install the root certificate on the Scanning Server:**

1. Connect to the Management Console via the web browser.
2. Navigate to Administration → System Settings → Finjan Devices.
3. Click the IP address.
4. Under Scanning Server right-click HTTPS and select Import Root Certificate. The following window appears:

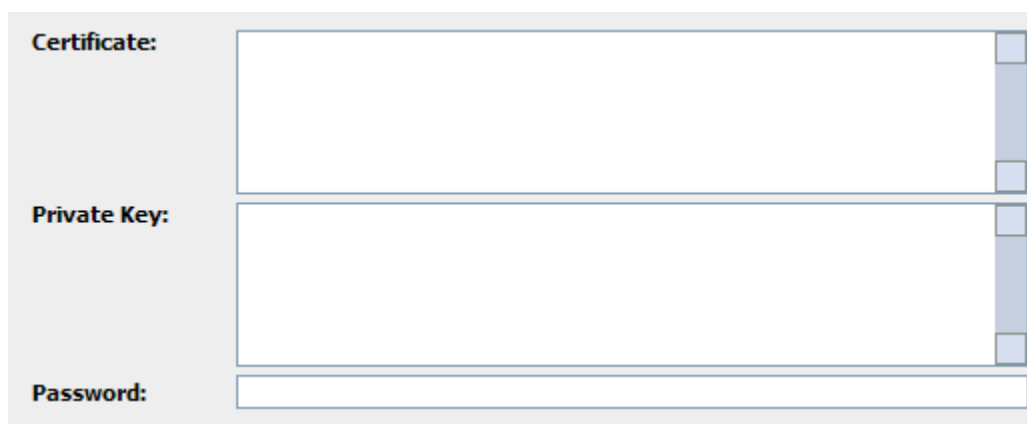


Figure 4 - Import Root Certificate

5. Paste the certificate and private key and type the password.
6. Click OK.



NOTE: For multiple Scanning Servers you can use the Device General Settings options instead of repeating the procedure on each Scanning Server.

3. HTTPS Policies

HTTPS Policies provide the option to define which HTTPS sites are scanned or blocked and which have content bypassing. The blocking mechanism is based on White Lists, URL categorization and checking to see if certificates have errors or comply with validation criteria.

Finjan provides two preconfigured HTTPS policies:

- ◆ **Default HTTPS Policy:** This Policy contains just one rule which is designed to block any sites that contain faulty certificates. Please refer to the Security Policies In-Depth manual for further information.
- ◆ **Default Emergency HTTPS Policy:** This was designed for emergency situations and contains two rules. The first rule allows only white list URLs and the second rule blocks the rest of the HTTP Traffic. This can be globally enabled via Policies → Default Policy Settings → Enable Emergency Policy checkbox.

In addition to the above two policies, the user can configure additional policies and rules. The security policies apply only to the way that the scanning server handles the certificate validation, bypassing scanning or blocking HTTPS traffic. Once traffic is decrypted, the Scanning Server scans the traffic based on the regular security policies, assigned to the users.

4. Configuring HTTPS Support

HTTPS scanning is a license based feature. HTTPS scanning enables decrypting HTTPS traffic and inspecting it for malicious code. It then re-encrypts the communication and sends it through to the end-user, ensuring clean content. Administrators can also set Bypass, Inspect Content and User Approval policies for encrypted traffic in order to remove the decision making from end-users.

The certificate validation functionality ensures that corporate policies for certificates are enforced by automatically validating each certificate and ensuring that the chain goes back to the trusted authority.

To configure HTTPS scanning, navigate in the Management Console to Administration → System Settings → Finjan Devices → HTTPS.

Device IP:

Enable HTTPS

HTTPS Service Advanced Allowed Server Ports

Listening IP: . .

Listening Port:

Figure 5 - HTTPS Configuration

4.1 HTTPS Configurable Parameters

System administrators can configure the following HTTPS related parameters.

4.1.1 HTTP Service

The following parameters can be configured by the administrator:

- ◆ Listening IP: For better system security, it is recommended to configure the IP address as the IP address of the corresponding physical interface.
- ◆ Listening Port: When working in explicit mode (proxy mode), this is the port number for the HTTPS scanning service.

4.1.2 Advanced

The following parameters can be configured by the administrator:

- ◆ Allow SSLv2: Enables support for SSLv2 protocol. This option is disabled by default. This protocol is non-secure and should not be used unless there are compatibility problems.
- ◆ Allow SSLv3: Enables support for SSLv3 protocol. This option is enabled by default.
- ◆ Allow TLSv1: Enables support for SSLv1 protocol. This option is enabled by default.
- ◆ Use Diffie-Hellman: Enables the use of Diffie-Hellman as the key exchange mechanism between the client and the proxy. This is enabled by default.
- ◆ Allow Weak Cipher Suites: Allows the choice of weak (non-secure) cipher suites while performing an SSL handshake between Vital Security and the HTTPS server. This option is disabled by default.
- ◆ Allow Certificate Wildcards: Allows support for Certificate Wildcards. The Certificate Wildcard works in conjunction with an existing Certificate Validation rule. This means that only if there is a policy with a Certificate validation rule will the wildcard support be relevant.

- ◆ SSL Handshake Timeout: Defines the amount of time (in seconds) after which the SSL Handshake is timed out if not responsive.
- ◆ Max HTTPS Transactions Backlog: Defines the maximum number of outstanding connection requests to be served by the system. After this number is reached, the system is timed out. The default value is 36.
- ◆ HTTPS Timeout: Defines (in seconds) the amount of time after which an idle connection is timed out.

Device IP:

Enable HTTPS

HTTPS Service Advanced Allowed Server Ports

Allow SSLv2

Allow SSLv3

Allow TLSv1

Use Diffie-Hellman

Allow Weak Ciphersuites

Allow Certificate Wildcards

SSL Handshake is seconds

MAX HTTP Transactions Backlog:

HTTPS Timeout is seconds

Figure 6 - HTTPS Advanced Settings

4.1.3 Allowed Server Ports

System administrators can configure which port numbers are allowed for HTTPS traffic. If the remote HTTPS server does not listen on the default TCP port number 443, other port numbers can be added.

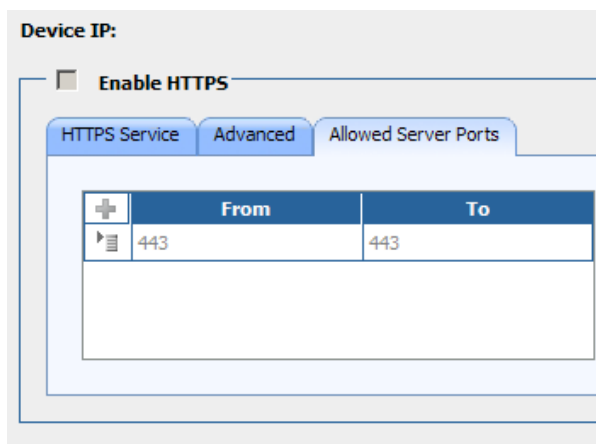


Figure 7 - Allowed Server Ports Settings

5. Transparent HTTPS

Vital Security version 9.0 introduces Transparent HTTPS Scanning. Transparent HTTPS Scanning allows system administrators to transparently redirect users to the Scanning Server, without the need to configure proxy settings for the users. This can be done by using one of the following methods:

- ◆ Layer 4 Switch: By using a third party layer 4 switch, it is possible to redirect all traffic, destined to port 443 (or any other port) to the Scanning Server.
- ◆ WCCP: By using a WCCP enabled router or switch, it is possible to redirect all traffic, destined to port 443 (or any other port) to the Scanning Server.
- ◆ Firewall Redirection: Some firewall vendors support the ability to transparently redirect traffic to third party vendors. In this case, a firewall policy can redirect all HTTPS traffic to the Scanning Server.



NOTE: User authentication is not supported in conjunction with Transparent HTTPS. User identification is based on the source IP address only.

5.1 Transparent HTTPS Scanning and Finjan's Certificate

Although HTTPS Scanning is transparent to the end user, it is still mandatory to install the SSL certificate of the Scanning Server on the end user's PC in order to prevent the security warnings. When the end user browses an HTTPS site, the Scanning Server generates on-the-fly certificate, signs the certificate and sends it to the end-user. If the user doesn't have the Scanning Server's certificate in the trusted CA's a warning message will appear.