

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 European Patent EP 0 965 094 B1 and U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968, 7058822, 7076469, 7155743, 7155744, 7185358, 7418731 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dote, Window-of-Vulnerability and RUSafe are trademarks or registered trademarks of Finjan. Sophos and Websense are registered trademarks of Sophos plc. McAfee is a registered trademark of McAfee Inc. Kaspersky is a registered trademark of Kaspersky Lab. IBM Proventia Web Filter is a registered trademark of IBM Corporation. SurfControl and Websense are registered trademarks of Websense, Inc. 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>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>	<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>For more information: Email: support@finjan.com Internet: www.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>

Catalog name: US-AU-ID-9.2

Table of Contents

1. Introduction	1
2. Identification and Authentication Overview	1
2.1 Gateway Device	3
2.2 User Identification Policy	3
2.3 User Authentication Process	5
3. User Management	9
3.1 User Import from LDAP Directories	10
3.2 Multiple LDAP Directories for the Same Domain	11
4. Configuration	12
4.1 Scanning Server Global Configuration	12
4.2 Gateway Device Global Configuration	15
5. Appendix A – NTLM Authentication on Windows Vista	23

1. Introduction

Enterprise networks are built from different topologies for which different device types and configurations are used. End-user identification and authentication can be performed via various tools, devices, and network equipment, and through the use of different protocols. The ability to identify the user during a Web transaction is crucial in order to isolate threats and enable policy enforcement with a specific behavior for each user or group. The option to identify and/or authenticate the user is dependent on the network layout, the security rules that are used in the network and the capability to integrate with an external password server (such as LDAP Directory). There is no common single solution that can fit all organizations, and, therefore, an enterprise solution should be flexible enough to offer support for multiple topologies.

Finjan's Vital Security Appliance comprises a flexible interface for supporting these topologies by providing a Web scanning interface that can be used either as a secured Web proxy server, as an ICAP server, or to scan end-user traffic transparently using WCCP. Additionally, Finjan's dedicated Gateway Devices can be used to isolate the local area network from the DMZ and perform direct access to an authentication server from a secured zone.

This document describes the identification and authentication capabilities as used while operating with the Vital Security Web security service as a proxy (explicit or transparent). It describes the identification and authentication methods used by Vital Security, including the various topologies available, as well as the setup and configuration procedures.

2. Identification and Authentication Overview

User identification is the process of identifying an end-user who is browsing via the Vital Security system for the following reasons:

Authorization – applying the correct policy to the end-user (for example, Security, Logging, and HTTPS policies)

Authorization – deciding whether a user is authorized to browse via the system

Auditing – Tracing end-user activity through logs, that is, recording (logging) transactions with details for future viewing and analyzing activities performed by the user

The User Identification process **does not** authenticate the user against the organization's password server. During the identification process, the end-users are requested to send their credentials (based on the identification scheme) to Vital Security, and the Vital Security system does not send the credentials to any other server.

In many cases, the end-user desktop runs in a Microsoft network environment in which the users are already authenticated. In such cases, the Vital Security

system must obtain the username/domain and match it with the users/groups list, which were previously imported from the organization's LDAP Directory. In other customer environments, mostly due to the fact that authentication causes a pop-up window to appear (non-Windows-based networks), user authentication is required to validate that the end-user is legitimate.

In both identification and authentication, users should be pre-provisioned in the Vital Security system to enable the system to identify and enforce the correct policy for them.

The following section summarizes the general differences between identification and authentication:

Identification – The end-user's browser initiates a Web session through Vital Security. Vital Security, at this point, can identify the user based on the source IP address or according to credentials, by challenging the user to send the credentials using NTLM or via clear text (basic authentication). If the second option is configured, an authentication handshake is performed between the end-user's browser and the Vital Security system, based on one of the pre-selected authentication types (basic or NTLM). If the user is already authenticated in the network, the end-user's browser will automatically send the required credentials to the VS system (In environments other than Windows, a pop-up window appears asking the user for credentials). Otherwise, a window dialog will pop up, requesting user credentials (username and password). Vital Security tries to locate the username in its pre-loaded users list (imported from AD/LDAP Directory). If the username is found, the policy that is assigned to the user will be enforced on that session (either a dedicated policy or a group policy). If the username is not found, the user will be assumed to be an unknown user and is given the security policy that is assigned to the Unknown Users group.

Authentication – Authentication is used when the user/domain information obtained from the end-user is validated via an external authentication server (for example, Active Directory). When real user authentication is required, the authentication is performed through the use of an authentication service running on one of the Finjan devices (Scanning Server or Gateway Device), which communicates with an authentication server to validate that the username/password supplied by the end-user's browser is actually participating in the supplied domain.

Using the Gateway Device to perform user authentication has four main benefits:

- Performance – The Scanning Server does not need to handle the entire authentication (which requires several HTTP transactions); therefore, the overall performance of the system is higher.
- Security – The Gateway Device is installed in the LAN, and all users' credentials remain in the LAN.
- High Availability and Scalability – The Gateway Device can be installed in a cluster (using a third-party load balancer) for high availability and scalability when better performance is required.

- Using the Gateway Device, it is possible to authenticate end-users against LDAP directories (while the Scanning Server supports only Active Directory).

2.1 Gateway Device

The Gateway Device provides a means to authenticate users in the Local Area Network (LAN) when Scanning Servers are installed in the Demilitarized Zone (DMZ). The Gateway Device acts as the proxy server for all end-users, and before the users begin browsing via the Vital Security system, it authenticates them. Based on the Identification Policy, the Gateway Device performs user authentication and sends the user's credentials to the password server. After successful authentication, it sends the traffic, in proxy format, to the scanning server.

Note: When there are multiple scanning servers, an external load balancing is required to load all the traffic that arrives from the Gateway Device.

The Gateway Device is located in the LAN, and when it performs the user authentication, it sends the credentials that were sent by the user to the password server, which is also installed in the LAN. In so doing, the end-user's credentials (password) remain in the LAN and do not leak into the DMZ.

The Gateway Device supports both the SMB protocol (when working with Microsoft Active Directory) and the LDAP protocol.

When the Gateway Device is used for authenticating end-users against Active Directory, it must be joined to the Domain.

2.2 User Identification Policy

Identification Policies carry out the classification of an end-user to determine whether the end-user should browse through the system. The Identification Policy also enables the system to enforce the proper Security Policy for the end-user. (After the end-user is identified or authenticated, a policy can be assigned to the specific user and user group.) The Identification Rules are based on both the type of authentication or identification that Vital Security uses and on lists of Header Fields, IP Ranges, Port Ranges, and URL Lists.

User identification in Vital Security is performed by obtaining the source IP of the connection and/or obtaining USER ID information (username/domain), and matching them with a pre-defined list of users which was imported from the LDAP Directory.

2.2.1 User Identification Rules

User Identification rules in Vital Security include the following:

Identify by Source IP – The user is identified according to the source IP address.

Identify by Headers – Vital Security reads HTTP headers supplied by a downstream proxy and identifies the user accordingly. This option is supported only by the Scanning Server.

Get User Credentials – Vital Security sends an authentication challenge requesting that the user send credentials. This option is supported only by the Scanning Server.

Authenticate – Vital Security performs complete user authentication. The end-user's credentials are sent to the password server for authentication.

When the Authenticate rule is selected, Vital Security supports the following password servers and authentication protocols:

Authenticated By	Supported Password Servers	Authentication Protocols
Scanning Server	SMB (Active Directory)	Basic/NTLM
Gateway Device	SMB and LDAP	Basic with LDAP NTLM with Active Directory

The Identification Policy and Authentication can be assigned to Vital Security Scanning Servers or Vital Security Gateway Devices. The device actions will be based on the policy assigned to it.

2.2.2 User Identification Conditions

User Identification conditions in Vital Security include the following:

Destination Port Range – Vital Security allows system administrators to perform user identification (and authentication) based on the value of destination port ranges. This condition allows bypassing authentication based on port ranges. For example, if there is a local application that uses a well-known port, using this condition, it is possible to bypass authentication when accessing that application. It is also possible to do the opposite, that is, authenticate users only when accessing that application.

Header Field – Using the Header Field conditions, Vital Security can authenticate or bypass authentication for pre-configured header fields. This condition can be useful when there is a need to bypass authentication for applications that do not support redirection, such as some types of media players or any other custom application.

IP Range – IP range allows system administrators to set rules according to the source IP ranges of the end-users.

URL Lists – System administrators can set different rules, based on the URL of the request. This can allow the administrator to configure the system in such a way that it will perform authentication only for specific URLs or bypass authentication based on the URL.

2.3 User Authentication Process

The User Authentication process differs on the Gateway Device and on the Scanning Server, and it differs when the authentication is transparent and when it is not.

2.3.1 Gateway Device Authentication Process

Since the Gateway Device acts as a proxy server for the end-users in the organization, the end-users send their requests to the Gateway Device. When the Gateway Device receives the initial HTTP request, it replies to the end-user with HTTP 407 – Proxy Authentication Required.

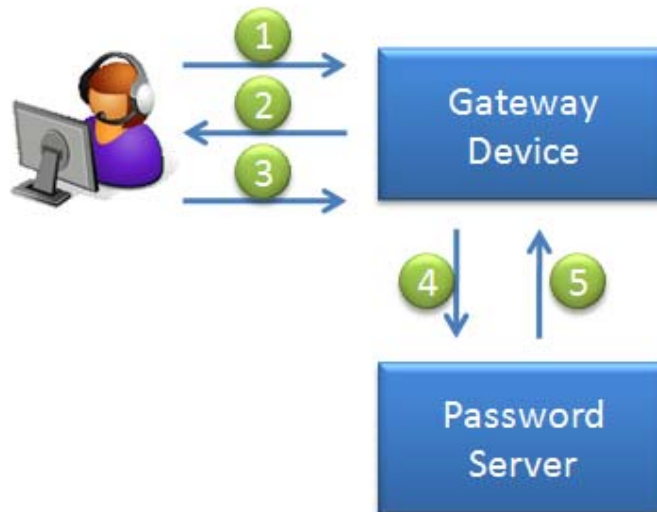


Figure 1 - User Authentication Process at the Gateway Device

Authentication Flow:

1. The end-user sends the HTTP request to the Gateway Device, which acts as the proxy server for the user.
2. The Gateway Device replies with HTTP 407 code – Proxy Authentication Required.
3. The end-user sends credentials to the Gateway Device.

4. The Device accesses the password server and authenticates the user.
5. When authenticating the end-user against the LDAP Directory, the Gateway Device performs BIND with the LDAP Directory using the credentials configured by the system administrator, followed by a second BIND using the credentials sent by the end-user.
6. When authenticating the end-user against Active Directory, the Gateway Device uses the proprietary SMB protocol to authenticate the user.
7. If the authentication is completed successfully, the end-user is allowed to browse via the system.

Notes:

When authenticating the end users against Active Directory, the Gateway Device must be joined to the domain.

Microsoft Active Directory 2008 is not supported.

Users with empty passwords cannot be authenticated by the Gateway Device.

2.3.2 Scanning Server Authentication in Transparent Mode

When the end-user sends the request to the Scanning Server and the Scanning Server is configured to perform user authentication, the Scanning Server responds with an HTTP 302 Redirect, which redirects the user to a virtual host. The virtual host is pre-configured, and its default value is vhost.finjan.com. The virtual host does not have to be a real host; however, the host name of the virtual host must be resolvable by the end-user. The end-user then closes the session and opens a new session for the virtual host (which does not actually exist). When Vital Security identifies a request for the virtual host, it knows that it must perform user authentication, and it responds to the end-user with HTTP 401 – Authentication Required. The end-user then sends the credentials, and the Scanning Server authenticates the end-user against the Active Directory.

Note: To prevent the authentication popup window, the virtual host should not include any dots in the host name in transparent mode. For example, the redirection host should be "vhost".

When the Scanning Server redirects the end-user to the virtual host, it also supplements the URL with the original URL that the end-user requested, in order to be able to redirect the user to the requested site.

When the authentication is completed, the Scanning Server redirects the end-user to the original address requested by the end-user.

The Scanning Server does not need to authentication each end-user request for a different Web site. The Scanning Server can retain the results of the authentication using different methods:

IP Caching – When IP caching is enabled, the Scanning Server treats all the sessions that arrive from the same IP address as if they were already authenticated.

Cookie Retention – When Cookie Retention is enabled, the Scanning Server adds a special cookie (encrypted) to each request from the same domain. In this case, the Scanning Server will perform authentication for different Web sites.

Note: When the Scanning Server is configured to work in Transparent mode, HTTPS authentication is not supported.

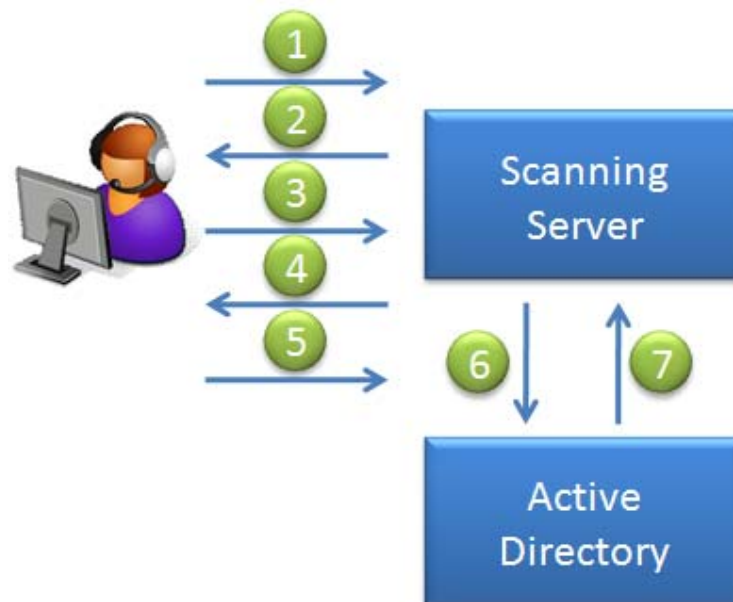


Figure 2 - Authentication Process in Transparent Mode

Authentication Flow:

1. The end-user sends the HTTP request to the Web server.
2. The Scanning Server intercepts the request and replies with the HTTP 302 redirect message. It then redirects the user to a pre-defined virtual host.
3. The end-user opens a new session with the virtual host.
4. When Vital Security sees the request to the virtual host, it replies with HTTP 401 – Authentication Required.
5. The end-user sends credentials to the Scanning Server.

6. The Scanning Server authenticates the users against the Active Directory Server.
7. If the authentication succeeds, Vital Security redirects the end-user to the original Web site.

2.3.3 Scanning Server Authentication in Proxy Mode

When the end-user sends the request to the Scanning Server, and the Scanning Server is configured to perform user authentication in Proxy mode, the Scanning Server responds with HTTP 407 – Proxy Authentication Required. The end-user then sends the credentials, and the Scanning Server authenticates the end-user against the Active Directory.

After successful authentication, the user is allowed to continue browsing via the Vital Security System.

The Scanning Server does not need to authentication each end-user request for a different Web site. The Scanning Server can retain the results of the authentication using different methods:

IP Caching – When IP caching is enabled, the Scanning Server treats all the sessions that arrive from the same IP address as if they were already authenticated.

Cookie Retention – When Cookie Retention is enabled, the Scanning Server adds a special cookie (encrypted) to each request for the same domain. In this case, the Scanning Server will perform authentication for different Web sites.

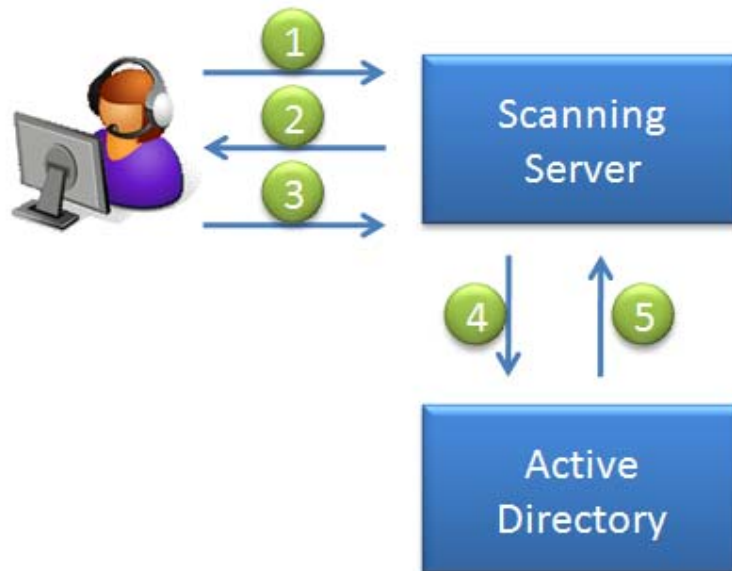


Figure 3 - Authentication Process in Proxy Mode

Authentication Flow:

1. The end-user sends the HTTP request to the Scanning Server, which acts as the proxy server for the end-user.
2. The Scanning Server replies to the end-user with HTTP 407 – Proxy Authentication Required.
3. The end-user sends credentials to the Scanning Server.
4. The Scanning Server authenticates the users against the Active Directory Server.
5. If the authentication succeeds, the user is allowed to browse via the system.

3. User Management

Vital Security classifies the end-users and applies the desired security policy according to the LDAP group to which the user belongs. Although it is possible to configure independent users and apply a dedicated security policy to them, user authentication is not supported for independent, as they are not imported from any LDAP Directory.

3.1 User Import from LDAP Directories

After the system administrator has configured the LDAP Directory, Vital Security imports a list of groups from it. The system administrator can choose which groups to import from the LDAP Directory into Vital Security.

	Go	Clear
<input type="checkbox"/> dom_mashina.com\Domain Computers		
<input type="checkbox"/> dom_mashina.com\Domain Controllers		
<input checked="" type="checkbox"/> dom_mashina.com\Domain Guests		
<input checked="" type="checkbox"/> dom_mashina.com\Domain Users		
<input type="checkbox"/> dom_mashina.com\Eli Group test.com		
<input type="checkbox"/> dom_mashina.com\Enterprise Admins		
<input type="checkbox"/> dom_mashina.com\Group Policy Creator Owners		
<input checked="" type="checkbox"/> dom_mashina.com\Group zaza		
<input checked="" type="checkbox"/> dom_mashina.com\Guests		
<input checked="" type="checkbox"/> dom_mashina.com\Guy's		

Page: 1 << Previous Next >>

Figure 4 - Selecting LDAP Groups

When the groups are selected, Vital Security imports the users who belong to those groups, and it then periodically imports the users into the system. The periodic import is required in order to update the users, in case users have been added to the groups or users have been moved from one group to another.

Users can be imported daily or every few hours, depending upon the configuration determined by the system administrators.

LDAP Import Schedule

Run daily at: 00:30

Run every: 2 hours

No Scheduled Import

Figure 5 – LDAP Import Schedule

Since a user may be part of more than a single group, the order of the groups in the LDAP screen has meaning. When one user belongs to two groups and each group is assigned to a different Security Policy, the system administrator can set the groups' priority by changing the display order.

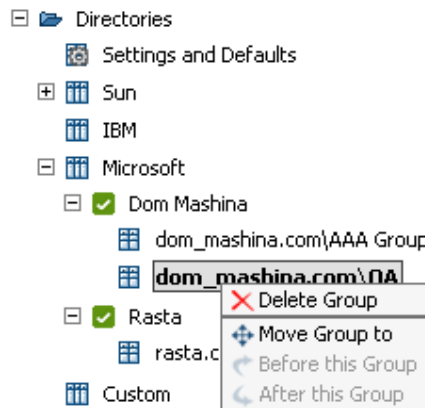


Figure 6 – LDAP Change Group Order

3.2 Multiple LDAP Directories for the Same Domain

In some cases, large enterprises employ multiple LDAP Directories, such that the primary LDAP Directory, housed in the corporate headquarters, contains information about the entire organization, and each branch also has an LDAP Directory, containing only a portion of the data (specifically about the users in the local branch) of the primary LDAP Directory. In such cases, Vital Security allows the system administrator to import all the users from the primary LDAP Directory and to use the local LDAP Directories in the remote branches for user authentication.

When multiple LDAP Directories are configured with the same Base DN and the same domain, the system administrator can select which LDAP is used for importing the entire users database into Vital Security.

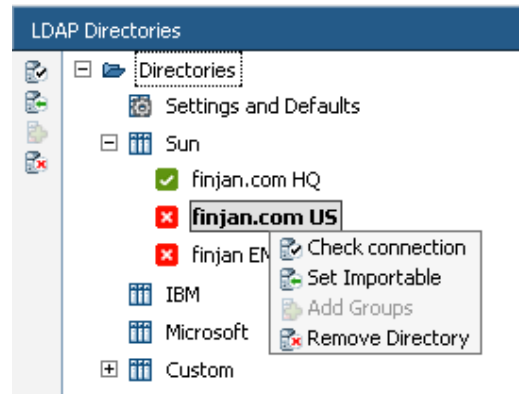


Figure 7 - Setting LDAP Directory as Importable

4. Configuration

The configuration of User Authentication requires the configuration of the following components:

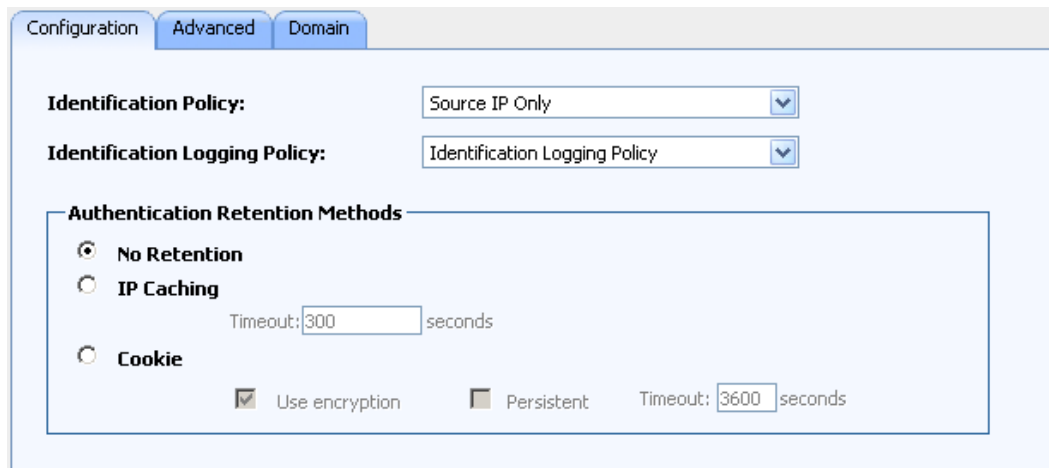
- The LDAP directory from which users are imported
- The Password server that is used by the Scanning Server or Gateway Device to authenticate the users
- The appropriate Identification Policies
- The Global Authentication settings

The User Authentication settings may be different based on the authentication scheme.

4.1 Scanning Server Global Configuration

The Global Authentication settings allow the system administrator to configure the following parameters:

4.1.1 Global Configuration



Configuration Advanced Domain

Identification Policy: Source IP Only

Identification Logging Policy: Identification Logging Policy

Authentication Retention Methods

- No Retention
- IP Caching
Timeout: 300 seconds
- Cookie
 Use encryption Persistent Timeout: 3600 seconds

Figure 8 - Scanning Server Global Configuration

Identification Policy – used by the Scanning Server to authenticate an end-user who is browsing via the Vital Security system

Authentication Retention Methods – When user authentication occurs, Vital Security has the ability to store the authentication result and not authenticate the end-user for each request.

4.1.2 Advanced Configuration

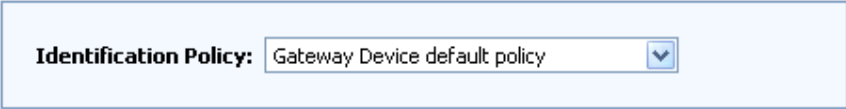
Figure 9 - Scanning Server Advanced Configuration

1. **Enabled Challenge Token Reuse (NTLM Settings)** – To save authentication time and proxy resources, the same token can be reused several times before a new random token is generated. A client authenticating with a proxy is provided with a Challenge Token, a random token that must be generated each time the NTLM Protocol is performed. Enabling this option allows Vital Security to reuse the same Challenge Token and reduce resource utilization. When this option is enabled, the system security level decreases.
 - **Random Challenge Token Reuse Number** – the number of times a Challenge Token can be reused (large values weaken the security level)
 - **Challenge Token Lifetime** – the time, in seconds, before Vital Security generates a new Challenge Token
2. **Active Directory Connection to Authentication Servers** – These parameters define timeouts and retries in case the Active Directory does not respond to the Scanning Server requests for authentication.
 - **Connection Timeout** – the timeout, in seconds, before the Scanning Server considers the Active Directory as Not in Service
 - **Try Reconnect After** – the timeout, in seconds, before the Scanning Server re-tries to connect to the Active Directory
3. **Transparent Authentication** – When Vital Security works in Transparent mode, it re-directs users browsing through the system to the host configured in the **Virtual Redirection Hostname**.

- **Virtual Redirection Hostname** – the host used to re-direct users. This host does not need to be a real host. The hostname configured in this field, however, must be resolvable by the DNS. (To prevent the authentication popup, the hostname must not include any periods.)
 - **Virtual Redirection Port** – the TCP port number used for re-direction
4. **Replace Domain With** – Occasionally, end-users do not send the domain imported from the LDAP Directory, and instead send the computer name (common for Novell eDirectory). When the end-user does not send the domain name, Vital Security fails to identify the user. When the Replace Domain With field is configured with the value of the domain and Vital Security fails to identify the user, Vital Security replaces the domain that was sent from the user with the value configured in this field. It then searches again for the user in the users list that was imported from the LDAP Directory.
 5. **Forward Upstream Proxy Authentication** – Enabling this option allows for an atypical situation in which an upstream proxy can authenticate users through the Vital Security system. This means that Vital Security will not perform authentication, but rather will forward proxy authentication from the downstream client. In this case, all Vital Security authentication mechanisms must be disabled.

4.2 Gateway Device Global Configuration

The global settings for the Gateway Device include the Identification Policy that is being used by the Gateway Device for user Authentication.



Identification Policy: Gateway Device default policy

Figure 10 - Gateway Device Authentication Settings

In addition to the Identification Policy, system administrators must also configure the upstream proxy of the Gateway Device, which can be either the IP address of the Scanning Server or a virtual IP address of a load balancer, which balances the traffic for the Scanning Servers.

HTTP Service				
Upstream Proxy				
Allowed Server Ports				
Protocol	IP Address	Port	Active	
HTTP	192 . 168 . 120 . 120	8080	<input checked="" type="checkbox"/>	<input type="checkbox"/> Use for all Protocols
HTTPS	192 . 168 . 120 . 120	8443	<input checked="" type="checkbox"/>	

Figure 11 - Gateway Device Authentication Settings

If Vital Security includes the Integrated SSL Scanning license, the HTTPS port should be port 8443 (or as configured on the Scanning Server). If Vital Security does not have a license for SSL scanning, the HTTPS port should be port 8080.

4.2.1 Transparent Authentication Configuration

The following is a step-by-step example of the configuration of the Scanning Server in order to perform user authentication in Transparent mode.

Prerequisites:

- Vital Security must be pre-configured with all relevant Security Policies.
- Transparent Scanning must be enabled.
- Microsoft Active Directory must be configured for users import.

⇒ **To Configure User Authentication**

1. To configure the Active Directory as the Password server, click **Users → Authentication Directories → Active Directory**. Add a new server and enter the information, based on the server's properties.

Realm/NETBIOS Name:

Active

Domain Controller:

+		Name
		192.168.100.100

Trusted Domain:

+		Name

Figure 12 - Configuring the Password Server

- To configure the Identification Policy, click **Policies → Identification**. To modify the Default Authentication Policy or expand the Authentication Policy, select the **Identify and Authenticate Users** rule and click **Edit**. Enable the rule by checking **Enable Rule** and selecting the domain configured in step 1 in the **Authentication Domain** dropdown menu.

Rule Name:

Description:

Enable Rule

Action:

Authentication Protocols:

Authentication Domain:

Figure 13 - Configuring Authentication Policy

- To configure Authentication, click **Administration → Finjan Devices → IP address** of the Scanning Server (or **Device Default Values → Scanning Server → Authentication**) and click **Edit**. From the Identification Policy dropdown menu, select the Identification Policy configured in step 2 (Authentication). Change the **Authentication Retention Method** to **IP Caching**. (the method used in this example).

Configuration **Advanced** Domain

Identification Policy: Authentication (Authenticate)

Identification Logging Policy: Identification Logging Policy

Authentication Retention Methods

No Retention

IP Caching
Timeout: seconds

Cookie
 Use encryption Persistent Timeout: seconds

Figure 14 - Configuring Authentication

- To configure the Virtual Redirection host, click the Advanced tab and change the value of Virtual Redirection Hostname to a short hostname with no periods (for example, vhost).

Configuration **Advanced** Domain

Enable Challenge Token reuse (NTLM Settings)
Warning! Enabling this feature decreases security.
Random Challenge Token reuse number:
Challenge Token lifetime is seconds


Active Directory Connection to Authentication Servers
Connection Timeout is seconds
Try Reconnect After is seconds

Transparent Authentication
Virtual Redirection Hostname
Virtual Redirection Port

Replace Domain With

Forward Upstream proxy Authentication

Figure 15 - Configuring Virtual Redirection Hostname

- Save the configuration and click  to commit changes.

4.2.2 Proxy Authentication Configuration

The configuration of User Authentication in Proxy mode is almost identical to the configuration of Transparent Authentication Configuration. The only

difference in terms of configuration is that step 4 of the Transparent Authentication Configuration example can be skipped. The default value of the Virtual Redirection Hostname is vhost.finjan.com, and this host can be resolved by the end-users. This field, however, can be changed to any other value, as long as it can be resolved by the end-users.

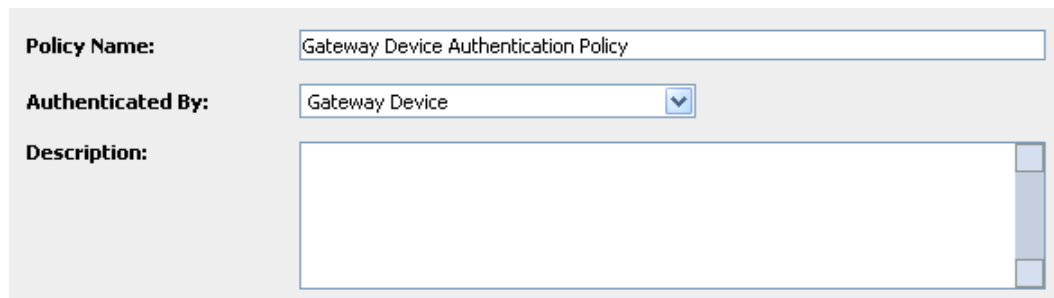
4.2.3 Gateway Device Configuration with LDAP Directory

Prerequisites:

- Vital Security must be pre-configured with all relevant Security Policies.
- LDAP directories must be configured on the Policy Server.

⇒ To Configure User Authentication

1. To configure the Authentication Policy, click **Policies → Identification** and create a new Authentication Policy. Assign a relevant name to the policy and select **Gateway Device** from the **Authenticated By** dropdown menu. Click **Save**.



The screenshot shows a configuration form for a Gateway Device Authentication Policy. It includes three main fields: 'Policy Name' with the value 'Gateway Device Authentication Policy', 'Authenticated By' with a dropdown menu set to 'Gateway Device', and a large empty 'Description' text area.

Figure 16 – Configuring Gateway Device Authentication Policy

2. To configure the Authentication Rule, select the policy added in step 1 and add a new rule. Enable the rule and set the Action to Authenticate. In the **Authentication Protocol** dropdown menu, select **Basic**. In the **Authentication Domain**, select the LDAP server used to perform the authentication.

The screenshot shows a configuration form for an authentication rule. At the top, there is a 'Rule Name' field containing 'Authentication Rule' and a larger 'Description' field which is currently empty. Below these fields, there is a section titled 'Enable Rule' with a checked checkbox. Underneath, there are three dropdown menus: 'Action' is set to 'Authenticate', 'Authentication Protocols' is set to 'Basic', and 'Authentication Domain' is set to 'Finjan LTD (LDAP)'.

Figure 17 – Configuring Gateway Device Authentication Rule

3. To configure the Gateway Device to use the Authentication Policy configured in step 2, click **Administration → System Settings → Finjan Devices** and select the IP address of the Gateway Device. Expand the Gateway Device configuration tree and select Authentication. Click **Edit** . In the Identification Policy, select the policy configured in step 2.

The screenshot shows a configuration form for an identification policy. It features a single dropdown menu labeled 'Identification Policy' which is currently set to 'Gateway Device Authentication Policy (Au)'.

Figure 18 – Configuring Gateway Device Identification Policy

4. To configure the Gateway Device to send traffic to the Scanning Server, click the HTTP node, then click the **Upstream Proxy** tab. Click **Edit** and specify the IP address of the Scanning Server.

Protocol	IP Address	Port	Active	
HTTP	192 . 168 . 120 . 120	8080	<input checked="" type="checkbox"/>	<input type="checkbox"/> Use for all Protocols
HTTPS	192 . 168 . 120 . 120	8443	<input checked="" type="checkbox"/>	

Figure 19 – Configuring Gateway Device Upstream Proxy

4.2.4 Gateway Device Configuration with Active Directory Server

The configuration of the Gateway Device for performing User Authentication against Active Directory is almost identical to the configuration of the Gateway Device with an LDAP Directory. The exception is that the Gateway Device must be joined to the domain.

⇒ To join the Gateway Device to the domain

1. To join the Gateway Device to the domain, click **Administration** → **System Settings** → **Finjan Device** and select the IP address of the Gateway Device. Right-click the IP address of the Gateway Device and select **Join**.

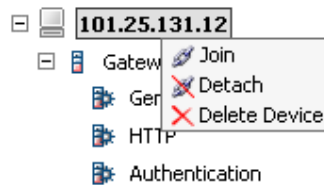


Figure 20 – Joining Gateway Device to Domain

2. Enter the parameters of the domain and click **OK**.

Figure 21 – Joining Gateway Device to Domain

- **Address** – the hostname or IP address of the Active Directory server.

- **DNS Domain Name** – the DNS name of the domain controller, for example, finjan.com
 - **User Name** – user name with privileges to add users to the domain
 - **Password** – the password of the authorized user
3. Proceed with step 1 of the Gateway Device Configuration with LDAP Directory example with the following exception:
- a. An Active Directory server must be pre-configured in the system.
 - b. The authentication protocol can be either NTLM or Basic.

5. Appendix A – NTLM Authentication on Windows Vista

Windows Vista, by default, does not negotiate NTLM versions when it performs user authentication; therefore an end-user who browses using Internet Explorer will fail to authenticate.

It is possible to configure Windows Vista to negotiate the NTLM version by using the following procedure:

1. Click the Windows Logo, select Run, and type “gpedit.msc”.

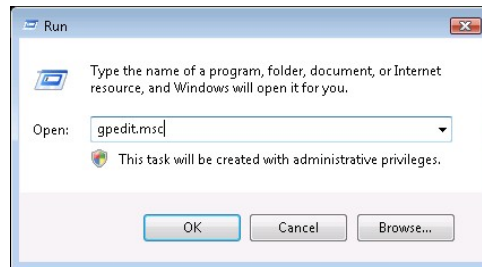


Figure 22 – Configure Windows Vista

2. In the **Group Policy Object Editor**, navigate to: Local Computer Company → Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options. In the right pane, search for **Network Security: LAN Manager Authentication Level** and double-click.

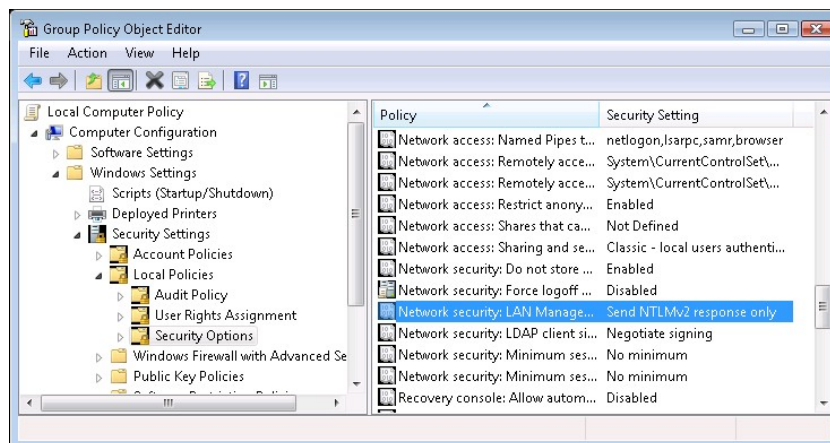


Figure 23– Group Policy Object Editor

3. From the Network Security: LAN Manager Authentication level, select **Send LM & NTLM – use NTLMv2 session security is negotiated**.

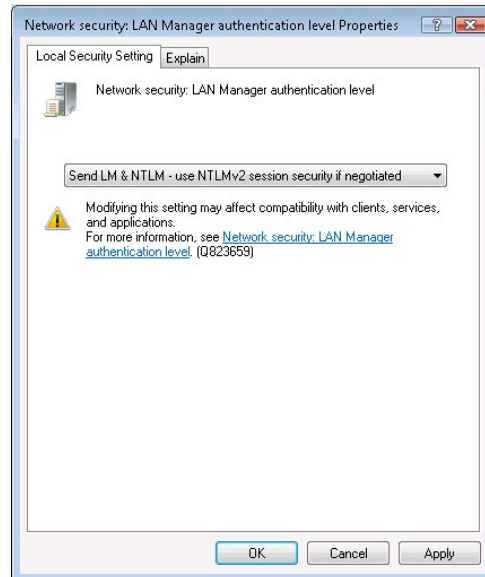


Figure 24– LAN Manager Authentication Level

4. Click **OK** and close the **Group Policy Object Editor**.