M86™ SECURITY

Security Policies In-Depth

Secure Web Gateway

Release 10.0 • Manual Version 1.01

M86 SECURITY POLICIES IN DEPTH

828 W. Taft Ave., Orange, CA 92865, USA

Version 1.01, published January 2011 for SWG software release 10.0

Every effort has been made to ensure the accuracy of this document. However, M86 Security makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. M86 Security shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

Trademarks

About This Manual

In this manual you will find a comprehensive description of the following policies and the rules within:

- M86 Master Policy
- M86 Basic Security Policy
- M86 Medium Security Policy
- M86 Strict Security Policy
- M86 HTTPS Policy
- M86 Emergency Policy
- M86 HTTPS Emergency Policy

Overview

M86 Security's **SWG Web Appliances** leverage synergies between the Active Content Behavior Based Profiles and other security engines (such as Anti-Virus, URL Filtering, HTTP headers filters, Vulnerability Anti.dote and more). These synergies are implemented in M86's rule-based system, which defines flexible sets of rules that describe expected cases and applies conditions on the content, and how the system should react in each case. Using these rules, each organization can create highly granular policies regarding the content/access allowed or forbidden for any single user or group of users, based on their responsibility and access rights.

M86 has designed several predefined Security and HTTPS Policies that you can edit at either a simplified level or on a more advanced level to tailor them to your organizational needs.

How to use this Manual

This manual provides you with an in-depth look at all the rules that comprise the Security and HTTPS Policies. For many of the rules, a rule demonstration has been provided, which enables you to test the rules in the system and subsequently monitor the Web Log view and transaction details afterwards. This involves you browsing through SWG and having various items of traffic scanned in accordance with your Security Policy. It is recommended to use the M86 Strict Security Policy for the rules demonstrations. You will also be guided through various rule demonstrations which show you how to add URLs to both Black Lists and White Lists - thereby blocking or allowing them respectively into your system.

Security Policies

Introduction to M86 Security Policies

The M86 SWG Policy is divided into two main components; **Master Policy** and **Security Policies**.

Master Policy

The purpose of the **Master Policy** is to provide the option to define a compulsory global policy for all groups within one organization. Only the Super Administrator has the right to change this policy. Administrators for different User Groups can only change the Policy or Rules that belong to their specific group.

NOTES: *A Master Policy can be comprised of any of the security policies from within the system. The Super Administrator can assign different Master Policies to different administrators or assign the same one to all administrators.*

The diagram below illustrates the relationships between the Super Administrators, Admnistrators, and the Security policies.

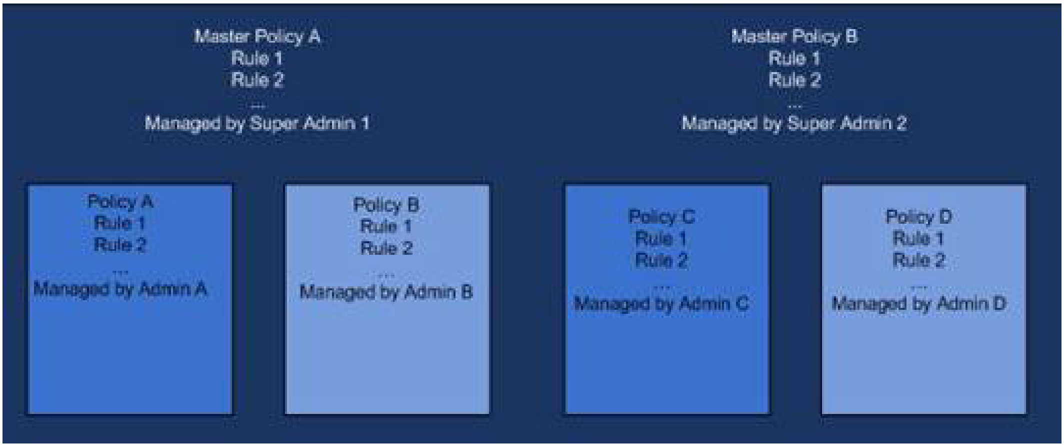


Figure 2-1: Master Policy Dependencies

Security Policies

M86 Security has designed three **Security Policies** intended to meet your individual organization's unique security needs.

- **M86 Basic Security Policy**: In this policy, only the basic engines for client web security are activated. This policy provides a baseline policy that can be used when connecting two relatively secure environments to each other.
- **M86 Medium Security Policy:** This policy builds on top of the basic security policy and adds more proactive, behavioral, real-time elements in order to provide better security when connecting to the internet. The policy uses all the security engines, and enforces the standard measures or code analysis. This is the default policy in the Management Console.
- **M86 Strict Security Policy**: This policy is used for higher sensitivity scenarios, where security cannot be compromised. It utilizes all the rules and standards for secure web behavior, while keeping HTML fixup enabled in order to still provide a usable browsing experience without blocking complete pages that may have violated some security standards.

NOTES: *These three default Policies are read only and maintained by M86.*

There are two adversely different ways of editing and configuring these Policies

Simplified Setup: Designed for busy customers; the Simplified Policies screen enables you to configure the level of protection your organization needs with the minimum of configuration effort. To find out more about Simplified Policies, please refer to the Management Console Reference Guide.

Advanced Setup: For more experienced system administrators, the Policies are comprised of both rules and conditions and can be duplicated and then heavily edited and tweaked from the main Policies tab.

HTTPS Policies are discussed in M86 HTTPS Policy.

Security Policy Rules Overview

The Policy rules are listed in order of priority from highest priority at the top to lowest priority at the bottom. Any action taken will be according to the rule of highest priority that matches a given transaction. After a rule is enforced, rules of lower priority are no longer relevant and are not evaluated.

Rules are composed of Conditions which act as building blocks and help set values on the content passing into your organization.

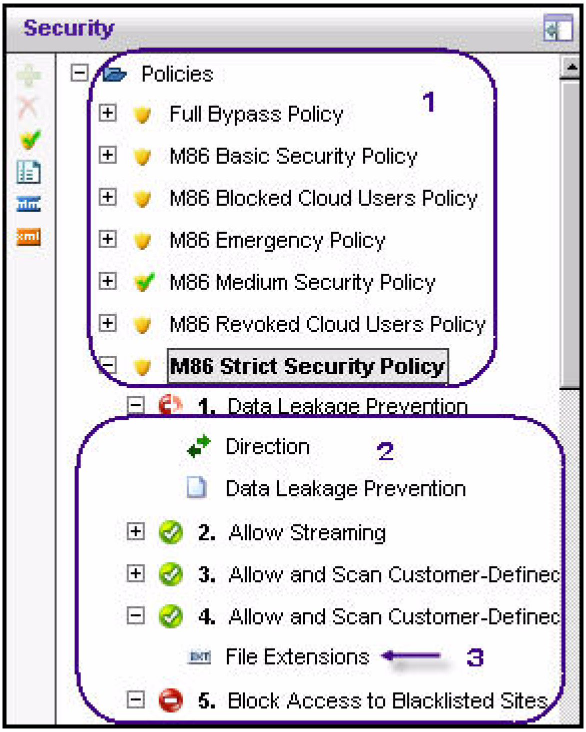
- One rule can include multiple conditions, **all** of which must be matched for the rule to be enforced. For example, a rule that includes conditions regarding file extensions, time frames and parent archive types, will be enforced only if all of the conditions are met.
- A Condition will be enforced even if only one of the selected options within a Condition is met.
- A rule has its level of priority depending on its position in the list. Rules can be moved up or down to change their position and priority level.
- If a rule is not specific to any of the listed values for the condition, instead of selecting all possible values, do not use the condition – leave it blank.
- All rules can be used in X-Ray mode, whereby a rule activity is logged but no action is taken. The rule activity is shown in the logs, and as such, a fine tuning or review of the rule (and its related policy) in the production environment will be possible.

For detailed illustrations of the X-Ray Security Policy, please refer to Appendix A:

Security Policy Hierarchy

The figure below details the hierarchy of security policies:

1. Polices Tree
2. Rules (in order of priority)
3. Rule Condition(s)



Security

Policies

1

Full Bypass Policy

M86 Basic Security Policy

M86 Blocked Cloud Users Policy

M86 Emergency Policy

M86 Medium Security Policy

M86 Revoked Cloud Users Policy

M86 Strict Security Policy

1. Data Leakage Prevention

Direction

2

Data Leakage Prevention

2. Allow Streaming

3. Allow and Scan Customer-Definec

4. Allow and Scan Customer-Definec

File Extensions

3

5. Block Access to Blacklisted Sites

Figure 2-2: Security Policies Screen (left tree pane)

The main screen displays policy details such as description and name.

Rule Process Method

The security rules are divided into two phases:

- **Request phase:**
  - If a **Block** action was triggered by a rule in the Request phase, the request will not be sent to the designated server, and an appropriate message will be displayed to the user.
  - If a **Coach** action was triggered by a rule in the Request phase, an appropriate message will be presented to the user. If the user then approves this message, the request will be sent to the designated server. The Coach action only applies to the Request phase and only for URL List or URL Categorization.
- **Response phase:**
  - The content received in the response phase (if any) will be evaluated regardless of the action taken in the request phase.
  - If an **Allow** action was triggered, the content is passed to the user. (Also - if no action was taken, the default action is an implicit Allow)
  - If a **Block** action was triggered, the content is not passed to the user. An appropriate error message is displayed.

When a **Master Policy** is being used (i.e. users will go through both a Master and a Security Policy) the rule process occurs as follows:

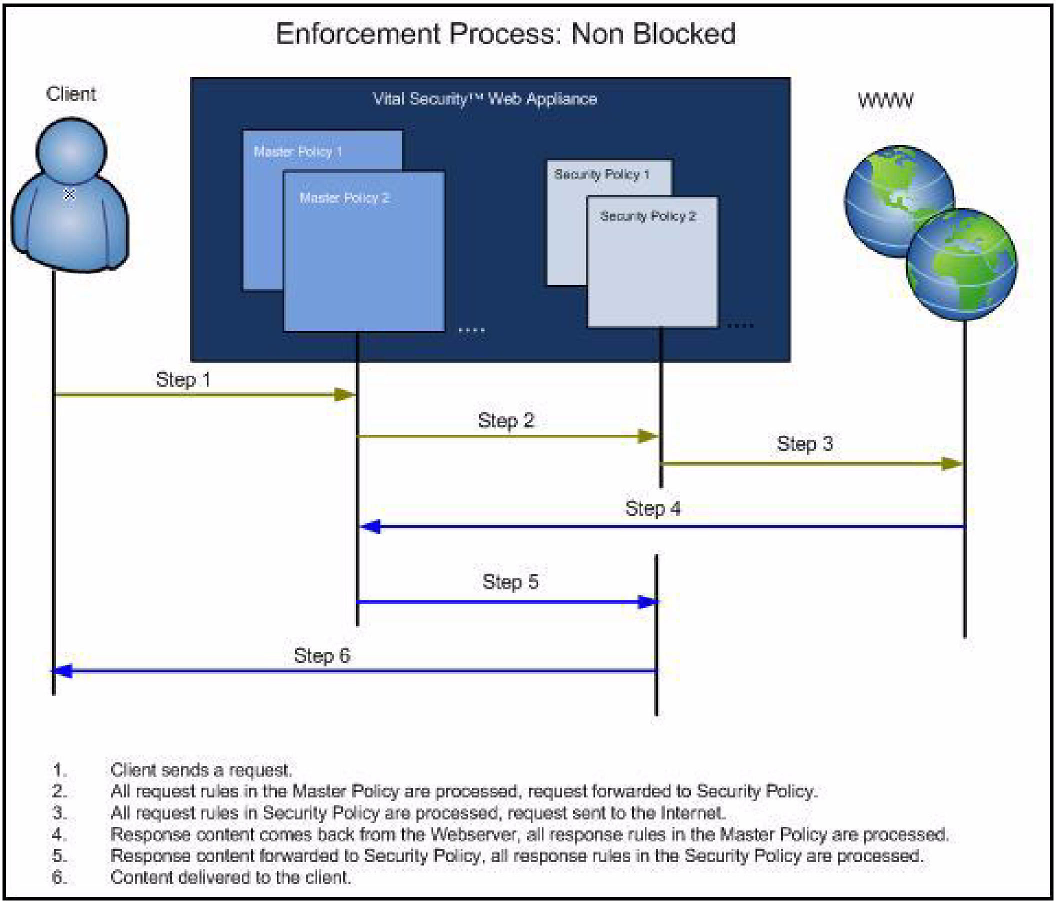
1. Client sends a request.
2. All request rules in the Master Policy are processed and the request is forwarded to the Security Policy.
3. All request rules in the Security Policy are processed and the request is sent to the Internet.
4. A response is returned from the Webserver.

5. All response rules in the Master Policy are processed, response content is forwarded to Security Policy.

6. All response rules in the Security Policy are processed and content is delivered to the Client

NOTES: *These rules are processed as long as a rule is not yet triggered.*

The diagram below illustrates the six primary steps in the rules transaction process detailed above:



1. Client sends a request.
2. All request rules in the Master Policy are processed, request forwarded to Security Policy.
3. All request rules in Security Policy are processed, request sent to the Internet.
4. Response content comes back from the Webserver, all response rules in the Master Policy are processed.
5. Response content forwarded to Security Policy, all response rules in the Security Policy are processed.
6. Content delivered to the client.

Figure 2-3: Rules Transaction Process

For more detailed diagrams of the Request and Reponse phases of the Master Policy and Security Policies interaction, please refer to Appendix A.

Rule Details

The Rules Details screen contains the following information with the option to make changes using the **Edit → Save/Cancel** options.

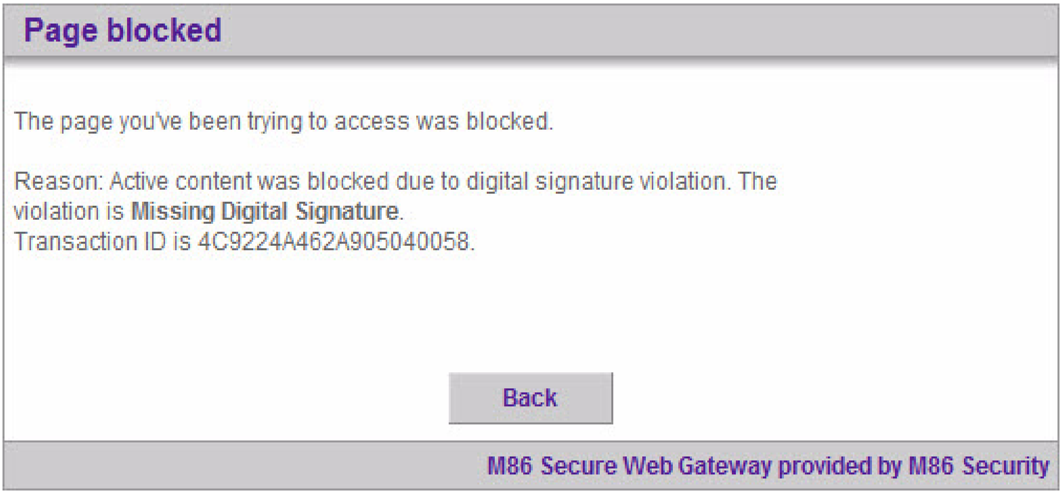
Field	Description
Rule Name	Defines the name of the Security rule.
X-Ray	If the X-Ray checkbox is checked, the rule is evaluated in the Logs only. In other words, an x-ray rule is activated and logged, but no block, warn or explicit allow action is taken.
Description	This provides a place for you to write a description of the rule.
Active When checked, the rule is active (enabled). When unchecked, the rule is disabled.	
Action: Block	The web content is blocked.
Action: Coach	The web content is temporarily blocked and the end-user receives a warning message that this site is not recommended and that his/her activities will be logged. The end-user can then decide whether to proceed or not
End-User Message	Defines which message is sent in the end-user blocked/coached message. The end-user message list and associated text is managed via Block?warn Messages. The end-user Message template can be modified via Message Template.

Field	Description
Do not send End-User Message	Withholds sending a **block** message to the end-user
Allow - Advanced Action	Three types of Advanced Allow Action are included: **Allow content and scan Containers**. The content is allowed, but container files are opened and the contents are scanned. (This is the default option) **Bypass Scanning** – Allows content through without any scanning at all on the request or response stage. This allows full streaming and is useful, for example, for sites which contain stock ticker streaming. **Allow content and don't scan Containers** – Allows content through including container files, such as zip or rar files, without scanning inside them. Content is allowed through on request stage but may be stopped on response stage.

Page Blocked Message

When an Internet site is blocked, a page block message (if configured) is sent to the end-user informing them that a site was blocked due to the relevant reason. This message also contains a transaction ID. Using the same transaction ID, the administrator can trace this transaction in the Log View and find out why this specific site/page was blocked.

An example of a Page Block message is as follows:



Page blocked

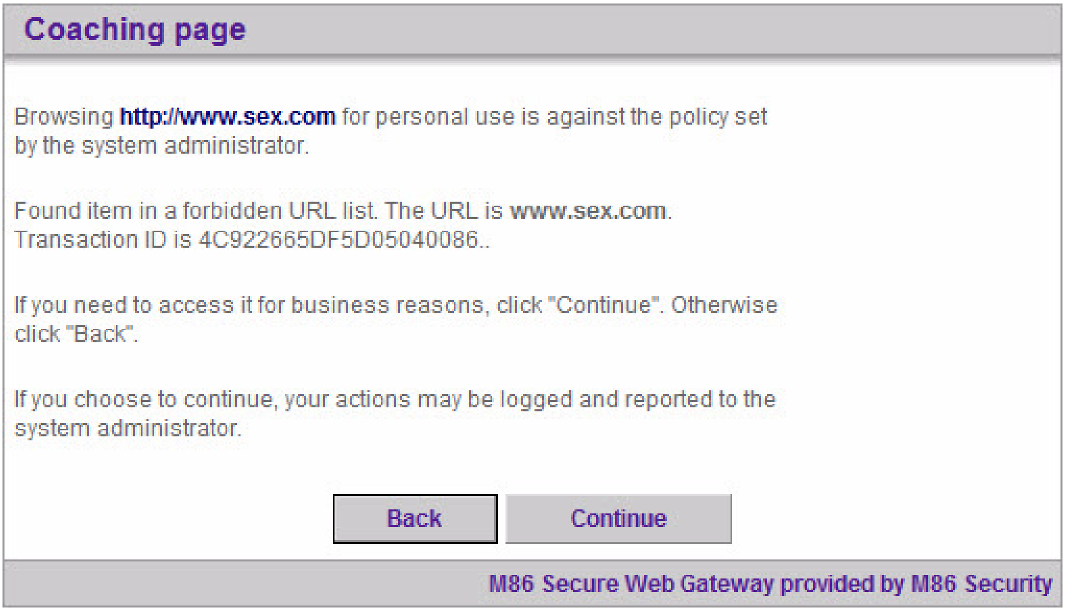
The page you've been trying to access was blocked.

Reason: Active content was blocked due to digital signature violation. The violation is **Missing Digital Signature**.
Transaction ID is 4C9224A462A905040058.

Figure 2-4: Example of a Page Block Message

Coaching Message (Warning)

An administrator can create a new Security Policy and within this Policy, create Coach (Warning) rules. This can be used as a warning for potential security situations or work performance loss for end-users. An example of a Coach message is as follows:



Coaching page

Browsing http://www.sex.com for personal use is against the policy set by the system administrator.

Found item in a forbidden URL list. The URL is www.sex.com. Transaction ID is 4C922665DF5D05040086..

If you need to access it for business reasons, click "Continue". Otherwise click "Back".

If you choose to continue, your actions may be logged and reported to the system administrator.

Figure 2-5: Example of a Coaching page

Partial Block Message

If part of the HTML page contains malicious code, SWG can remove that specific part of the HTML page and allow the rest of it to be displayed to the end-user.

Conditions

Each rule may include multiple **Conditions**; all of which must be met in order for the rule to be followed. The following Conditions are available:

- **Active Content List** – The Active Content List condition contains active content objects such as ActiveX Controls and Java Applets which have already been scanned by SWG and kept in the SWG Server Database. Each newly scanned Applet, Control or Executables will be automatically added to the Auto-generated list, which is the only list that cannot be used in a rule. Items from the Auto-generated list may be moved to other lists in order to create exception rules. The condition will apply to objects that match entries in these lists.SWG includes the following default lists which can be used as part of this condition:
    - **Allowed** – Allows trusted objects which are blocked by the Default Security Policy.
    - **Blocked** – Blocks forbidden objects which are allowed by the Default Security Policy.
    - **Spyware objects** – Contains known spyware profiles in a non-editable list predefined by M86. This is not viewable.
    - **Unscannable** – This list is automatically populated by items that the appliance failed to scan.
- **Anti-Virus (McAfee/Sophos/Kaspersky)** – Anti-Virus third party scanning engine which scans for known viruses.
- **Archive Errors** – This applies if an archive is not scanned by SWG due to predefined conditions such as: password protection, nesting depth, expanded file exceeding limit, file could not be extracted, etc.
- **Behavior Profile (Binary)** – Behavior Profiles which define behaviors that could be considered malicious or suspicious when exhibited by ActiveX Controls, Java Applets, executable files and any other relevant files. These are configured in the **Security Engines** tab of the Management Console. This

condition can also match objects to the following non-editable profiles:

  - **Suspected Malware** – This option only appears if the Anti-Spyware engine is purchased. It contains behavior profile patterns that are specific to Spyware objects.
  - **Unscannable Active Content** – This profile will be assigned whenever the appliance could not scan an object.

- **Behavior Profile (Script)** – Behavior Profiles define behaviors that could be considered malicious or suspicious when exhibited by Web pages, VB Script files, Java Script files and other relevant files. This condition also includes the Vulnerability Anti.Dote profiles. All these profiles are configured under the **Security Engines** tab of the Management Console. This condition can also match objects to the following non-editable profiles:
  - **Spyware Profile** – It contains behavior profile patterns that are specific to Spyware objects.
  - **Unscannable Active Content** – This profile will be assigned whenever the appliance could not fully scan an object.
- **Binary VAD -** The Binary Vulnerability Anti.dote (VAD) condition scans binary files, looking for patterns of exploits.
- **Content Size** – Specifies the content size range. For example, using this condition, one might apply a rule only to content size over 10MB. Traffic management cannot be carried out based on content size as the Appliance always downloads the full content first.
- **Digital Signatures** – Specifies if the content has a digital signature which is invalid for a number of reasons, or is missing.
- **Direction** – Specifies the direction of the transaction (Incoming/ Outgoing) for which the rule may be triggered. For example, in HTTP, Outgoing means the request phase, and Incoming means the response phase of the protocol. If no direction is specifically applied – then the rule is checked on both the request and response phases.

- **File Extensions** – Refers to the ‘declared’ content type, i.e. the file extension. It also detects potentially malicious extensions such as multiple extensions (e.g. **example txt.exe**).
- **Header Fields** – This rule condition applies to requests and responses which contain a selected HTTP header.
- **IM** – This condition applies to transactions using Instant Messaging protocols with HTTP tunnelling.
- **Parent Archive Type** – This condition allows the administrator to assign specific rules for items within archives such as ZIP, CAB, etc. This condition will not match files outside of archives or the archive files themselves.
- **Protocol** – This condition covers the different protocols used for browsing or downloading.
- **Spoofed Content** – This condition applies to malicious files disguised as harmless files.
- **Static Content List** – This condition applies if a content's signature is found in a list of predefined malicious content signatures. This list is invisible to the administrator, and is constantly updated by M86's Malicious Code Research Center (MCRC).
- **Time Frame** – This condition contains the time frame(s) during which this rule should be applied (e.g. Weekend, Lunch)
- **True Content Type** – Unlike the declared content type, the True Type detection engine limits the rule action to predefined content types. The engine uses real content inspection to identify the type of the content.
- **URL Filtering (Websense/IBM)** – Specifies which URL category (or categories) the rule should apply to. These categories are maintained by the respective 3rd party.
- **URL Lists** – This condition refers to lists of URLs that have been defined in the List Management tab in the Management Console. This condition can also match the following non-editable list: Spyware URL List. This option contains a list of known Spyware sites.

M86 Security Policies - Advanced

In the Advanced Policies tab - the Security Policy rules themselves cannot be edited (unless you duplicate the policy). However, some of the Conditions - such as URL Lists - can be edited through **Policies → Condition Settings**, thereby changing your Security Policy.

M86 Basic Security Policy Rules

The following rules are used in the M86 Basic Security Policy:

Allow Streaming

Allow and Scan Customer-Defined True Content Type

Allow and Scan Customer-Defined File Extensions

Block Access to Blacklisted Sites

Block Access to Spyware Sites

Block Access to Adware Sites

Allow Trusted Sites

Customer-Defined URL Filtering (Websense/IBM)

Data Leakage Prevention

Block Access to High-Risk Site Categories (Websense/IBM)

Allow Known Legitimate Content

Allow Whitelisted ActiveX, Java Applets and Executables

Block ActiveX, Java Applets and Executables by ACL

Block Known Spyware (CLSID)

Block Known Spyware (ACL)

Block Potentially Malicious Archives

Block Binary VAD Vulnerabilities

Block Known Viruses (McAfee / Sophos / Kaspersky)

Block Customer-Defined File Extensions

Block Customer-Defined True Content Type

Block Known Malicious Content

Detect Known Trojan Network Activity

Allow Access to White Listed Sites

Block Binary Objects with Invalid Digital Certificate

Block Application Level Vulnerabilities

Block Illegitimate Archives (Including Password-Protected Archives)

M86 Medium Security Policy Rules

The following rules are used in the M86 Medium Security Policy:

Allow Streaming

Allow and Scan Customer-Defined True Content Type

Allow and Scan Customer-Defined File Extensions

Block Access to Blacklisted Sites

Block Access to Spyware Sites

Block Access to Adware Sites

Allow Trusted Sites

Customer-Defined URL Filtering (Websense/IBM)

Block Access to High-Risk Site Categories (Websense/IBM)

Allow Whitelisted ActiveX, Java Applets and Executables

Block ActiveX, Java Applets and Executables by ACL

Block Known Spyware (CLSID)

Block Known Spyware (ACL)

Block Potentially Malicious Archives

Block Binary VAD Vulnerabilities

Block Known Viruses (McAfee / Sophos / Kaspersky)

Block Known Malicious Content

Block IM Tunneling

Detect Known Trojan Network Activity

Block Microsoft Office Documents containing Macros and/or Embedded Files

Block Binary Exploits in Textual Files

Allow Access to White Listed Sites

Block Spoofed Content

Block Outgoing Microsoft Office Documents

Block Files with Suspicious Multiple Extensions

Block Blacklisted File Extensions

Block Files with COM Extensions

Block Unscannable Archives

Block Potentially Malicious Packed Executables

Block Binary Objects without a Digital Certificate

Block Binary Objects with Invalid Digital Certificate

Block Customer-Defined True Content Type

Block Suspicious File Types

Block Application Level Vulnerabilities

Block Malicious Scripts by Behavior

Block Malicious ActiveX, Java Applets and Executables

Block Illegitimate Archives (Including Password-Protected Archives)

Block Unscannable ActiveX, Java Applets and Executables

Block Unscannable Web Pages and Scripts

Block Unscannable (McAfee / Sophos / Kaspersky)

IMPORTANT: *The difference between the Medium and Strict Security Policies is displayed in the Block Unscannable ActiveX, Java Applets and Executables rule where the Default Profile - Binary Behavior is not blocked in the Medium Security Policy.*

M86 Strict Security Policy Rules

The following rules are used in the M86 Strict Security Policy:

Data Leakage Prevention

Allow Streaming

Allow and Scan Customer-Defined True Content Type

Allow and Scan Customer-Defined File Extensions

Block Access to Blacklisted Sites

Block Access to Spyware Sites

Block Access to Adware Sites

Allow Trusted Sites

Customer-Defined URL Filtering (Websense/IBM)

Block Access to High-Risk Site Categories (Websense/IBM)

Allow Whitelisted ActiveX, Java Applets and Executables

Allow Known Legitimate Content

Block ActiveX, Java Applets and Executables by ACL

Block Known Spyware (CLSID)

Block Known Spyware (ACL)

Block Potentially Malicious Archives

Block Binary VAD Vulnerabilities

Block Known Viruses (McAfee / Sophos / Kaspersky)

Block Known Malicious Content

Block IM Tunneling

Detect Known Trojan Network Activity

Block Microsoft Office Documents containing Macros and/or Embedded Files

Block Binary Exploits in Textual Files

Block Spoofed Content

Block Outgoing Microsoft Office Documents

Block Files with Suspicious Multiple Extensions

Block Blacklisted File Extensions

Block Files with COM Extensions

Block Unscannable Archives

Block Potentially Malicious Packed Executables

Block Binary Objects without a Digital Certificate

Allow Access to White Listed Sites

Block Binary Objects with Invalid Digital Certificate

Block Customer-Defined True Content Type

Block Suspicious File Types

Block Application Level Vulnerabilities

Block Malicious Scripts by Behavior

Block Malicious ActiveX, Java Applets and Executables

Block Illegitimate Archives (Including Password-Protected Archives)

Block Unscannable ActiveX, Java Applets and Executables

Block Unscannable Web Pages and Scripts

Block Unscannable (McAfee / Sophos / Kaspersky)

IMPORTANT: *M86 MCRC have provided Rule Demonstrations where possible for the above rules. Before beginning the Rule Demonstrations:*

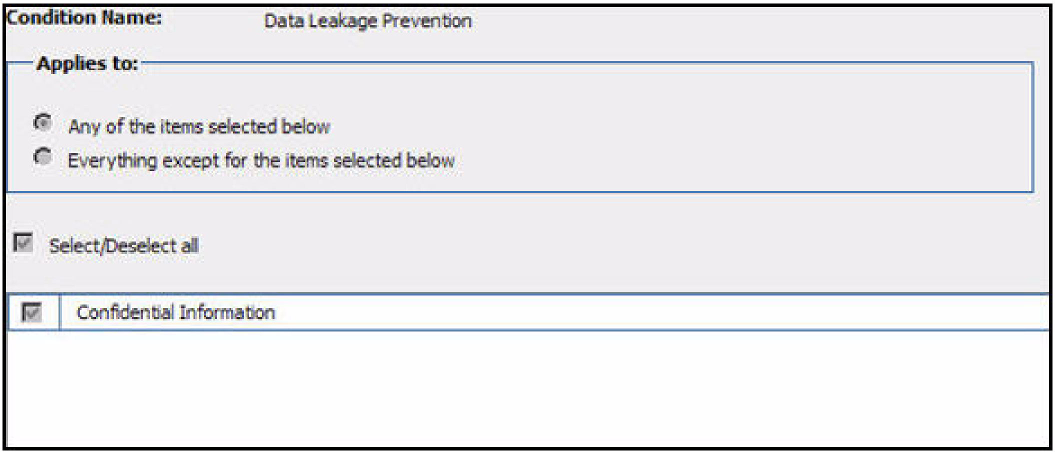
1. Ensure that your browser is configured with the SWG NG Appliance IP as an HTTP proxy.

2. Disable HTML Repair: Navigate to **Administration → Scanning Options** *and deselect the* **Automatic Removal of Suspicious code** *checkbox.*

Security Policy Rules

Data Leakage Prevention

The **Data Leakage Prevention** (X-Ray default) rule was designed to scan web content in order to prevent vital information from leaving the company network.



Condition Name: Data Leakage Prevention

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

☑ Select/Deselect all

☑ Confidential Information

Figure 3-1: Data Leakage Prevention Condition Screen

The following table displays the Rule Editor definitions.

Block Data Leakage Prevention	
Action	Block, Allow, or Coach
End-User Message	Data Leakage Prevention
Conditions	

Block Data Leakage Prevention	
Direction	This condition allows the administrator to trigger a rule specifically on the request (Outgoing) or response (Incoming) phase of the transaction.
Data Leakage Prevention	This condition allows the administrator to monitor and prevent data leakage.

Further Information:

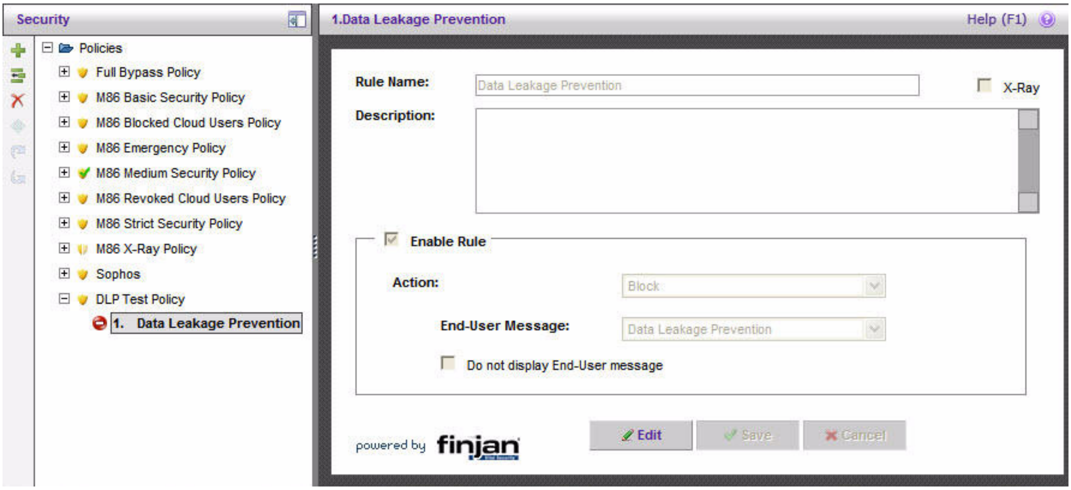
The **Data Leakage Prevention** rule refers to the **Data Leakage Prevention** profile which can be found via **Policies → Condition Settings → Data Leakage Prevention.**

Rule Demonstration:

Test the Behavior Profile rule with the following file examples:

➲ **Example 1: Create a new Data Leakage Prevention Rule**

1. In the Management Console navigate to **Policies → Security → Advanced** to create a new Security Policy.
2. In the right window pane, name the policy **DLP Test Policy.** Click **Save**.
3. Create a new rule by clicking ✚ on the left panel. Name it “Data leakage prevention” and select “Data Leakage Prevention” as the end user message:


Security
Policies
Full Bypass Policy
M86 Basic Security Policy
M86 Blocked Cloud Users Policy
M86 Emergency Policy
M86 Medium Security Policy
M86 Revoked Cloud Users Policy
M86 Strict Security Policy
M86 X-Ray Policy
Sophos
DLP Test Policy
1. Data Leakage Prevention
1.Data Leakage Prevention
Help (F1)
powered by finjan
Edit
Save
Cancel

Rule Name: Data Leakage Prevention

☐ X-Ray

Description:

☑ Enable Rule

Action: Block

End-User Message: Data Leakage Prevention

☐ Do not display End-User message

Figure 3-2: Create New Rule

Create a new DLP condition

The following condition provides an example of how to block documents with credit card numbers as part of the content.

In the Management Console, navigate to **Policies → Condition Settings → Data Leakage Prevention**.

1. To create a new Filter Condition, right-click the Data Leakage Prevention node and select **Add Filter Condition.** (The left toolbar offers the same action by clicking ✚)

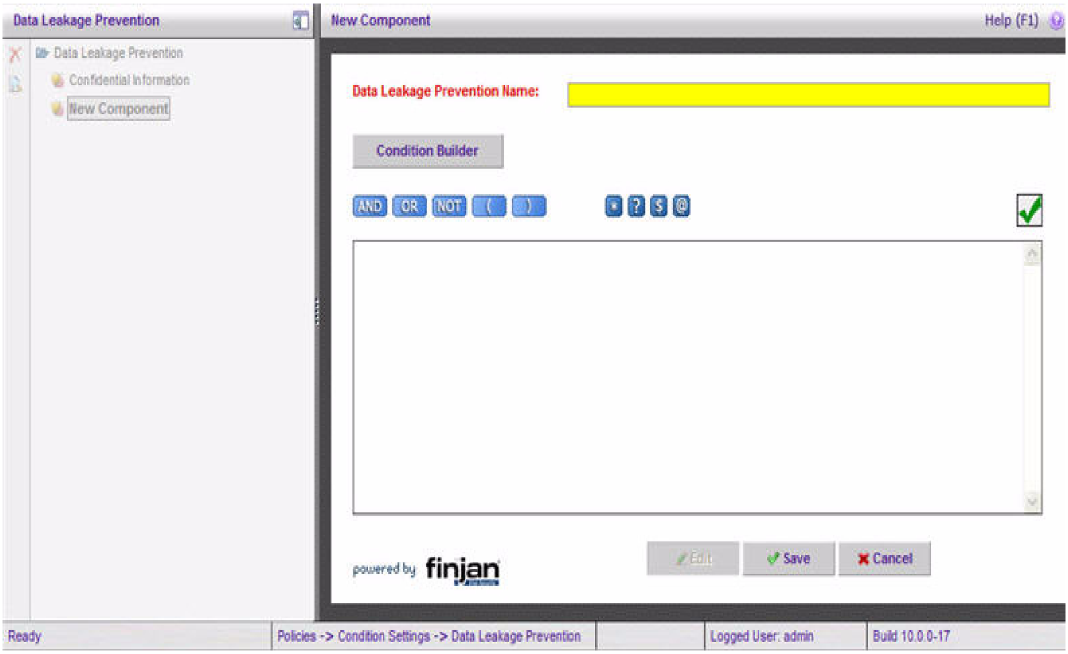


Figure 3-3: Create New Filter

2. In the New Component window, enter an appropriate Condition Name in the Data Leakage Prevention Name field (for example, Block Documents with Diners CC).

➲ To Edit in Condition Editor mode:

a Create new filter condition, and set the name to “Block Documents with Diners CC”.

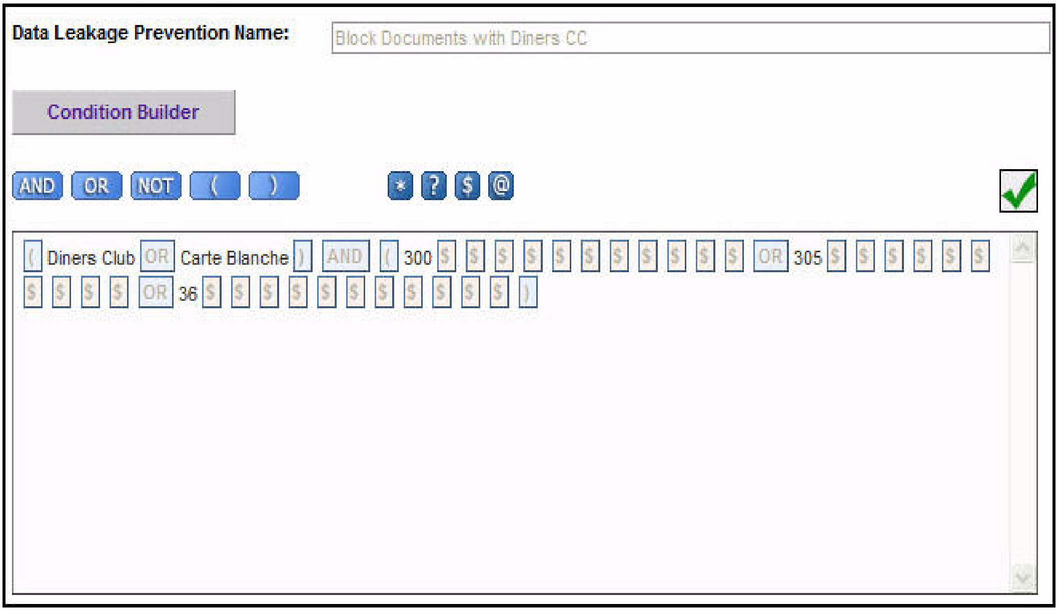
b Build the condition using the available values, placeholders, and operators.

c For this example, build the following condition (as shown in the following screenshot): (Diners Club OR Carte Blanche) AND (300$$$$$$$$$$$ OR 305$$$$$$$$$$$ OR 36$$$$$$$$$$$$)

d (Diners Club OR Carte Blanche) AND (300$$$$$$$$$$$ OR 305$$$$$$$$$$$ OR 36$$$$$$$$$$$$)

NOTES: *Be sure to use the placeholders buttons for the right and left parentheses, the "OR" and "AND" logical operators, and the $ numerical wild card.*

e Click **Save**.



Data Leakage Prevention Name: Block Documents with Diners CC

(Diners Club OR Carte Blanche) AND (300 $ $ $ $ $ $ $ $ $ $ $ OR 305 $ $ $ $ $ $ $ $ $ $ OR 36 $ $ $ $ $ $ $ $ $ $ $)

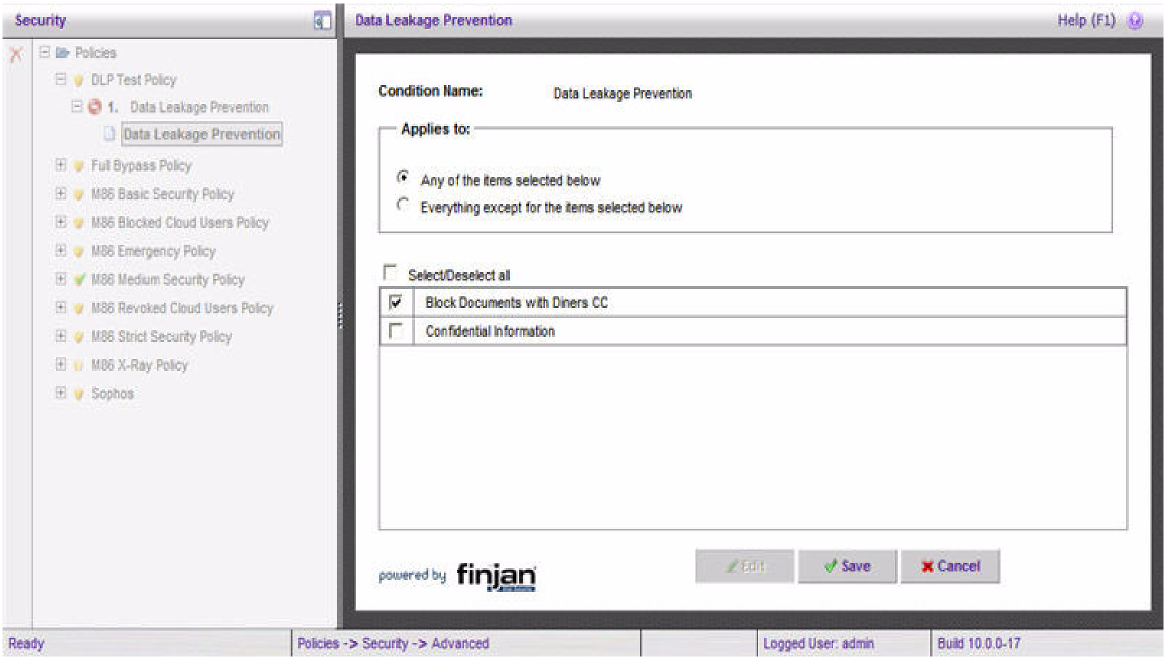
Figure 3-4: Condition Builder Placeholders

NOTES: *This can also be performed using the Condition Builder.*

The previous images provide an example of a condition created to ensure that Diner's Club credit card numbers do not leave the company. For example, an entry such as Diners Club 3005 458696 5454 is recognized and blocked, since credit card information representative of Diners Club (such as a number beginning with 300 and a total of 14 digits) is recognized. However, an entry such as Diners Club 4005 458696 5454 will not be blocked, as it does not meet the condition requirements (such as the number 300) and is therefore known not to be a valid Diners Club credit card number.

➲ Assigning Conditions to Policy Rules:

1. Navigate in the Management Console to **Policies → Security → Advanced**, and select the **DLP Test Policy**.
2. Expand the policy and select the Data Leakage Prevention rule.
3. Add a new condition to the rule by clicking ✚ in the left toolbar. Set the condition name to “Data leakage prevention” and enable the checkbox near the “Block Documents with Diners CC” entry.



Condition Name: Data Leakage Prevention

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

☑ Block Documents with Diners CC
□ Confidential Information

Figure 3-5: Assigning Conditions

4. Click **Save**.

5. To ensure that the new policy is in use, navigate to **Policies → Default Policy Settings** and select “DLP Test Policy” as the default security policy.

Testing the new rule:

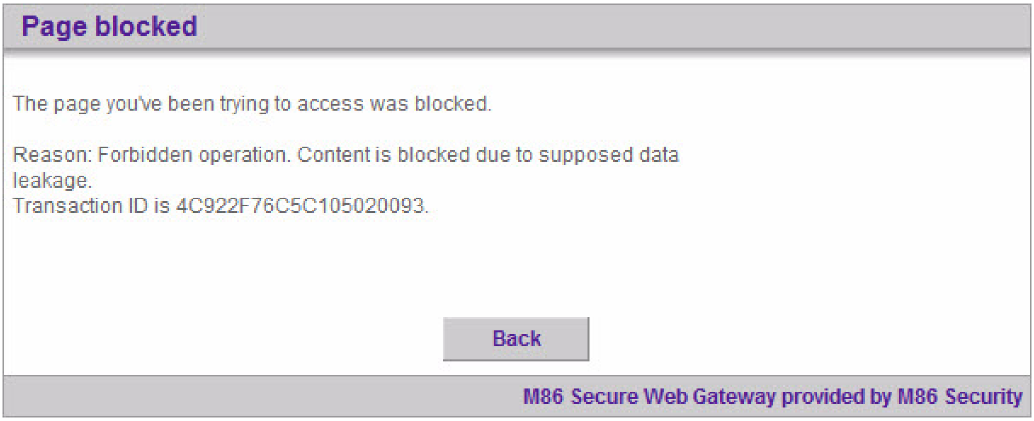
1. Copy and paste the following URL into your browser:

http://www.m86security.com/EVG/diners.doc

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.
3. Copy and paste the following URL into your browser:

http://www.m86security.com/EVG/data_leakage_test.asp

4. Click on Browse and select the file “diners.doc” downloaded previously.
5. Click **Upload.**
6. If everything was set correctly, you should receive a blocking message similar to the following:



Page blocked

The page you've been trying to access was blocked.

Reason: Forbidden operation. Content is blocked due to supposed data leakage.
Transaction ID is 4C922F76C5C105020093.

Figure 3-6: Data Leakage Prevention Page Block Message

➲ Example 2: Test Rule

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/confidential.doc

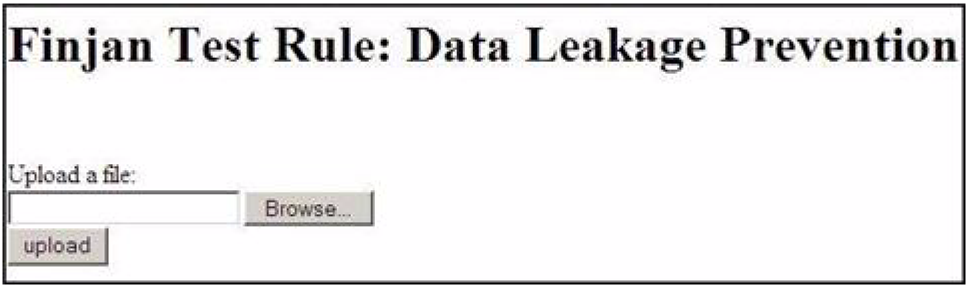
   This link will download a file containing the word "confidential"

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**and click **OK**.

3. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/data_leakage_test.asp

The following page appears:



Finjan Test Rule: Data Leakage Prevention

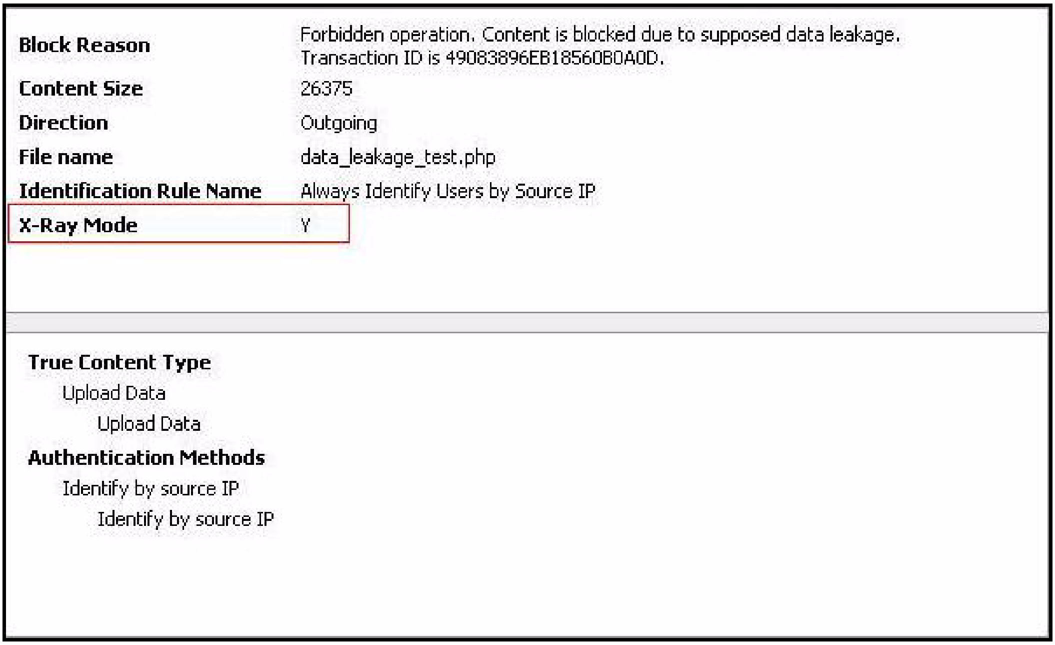
Upload a file:

Figure 3-7: Test Rule for Data Leakage Prevention

4. Click on Browse and select the file **confidential.doc** downloaded previously.
5. Click **Upload**.
6. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation toolbar.
7. In the same row as the blocked transaction, click and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

8. In the Transaction Details tree, click Request/Response to obtain further information on the Request and Response phases of this transaction.

9. Click Request



Block Reason	Forbidden operation. Content is blocked due to supposed data leakage. Transaction ID is 49083896EB18560B0A0D.
Content Size	26375
Direction	Outgoing
File name	data_leakage_test.php
Identification Rule Name	Always Identify Users by Source IP
X-Ray Mode	Y

True Content Type
- Upload Data
  - Upload Data

Authentication Methods
- Identify by source IP
  - Identify by source IP

Figure 3-8: Content Blocked Due To Supposed Data Leakage

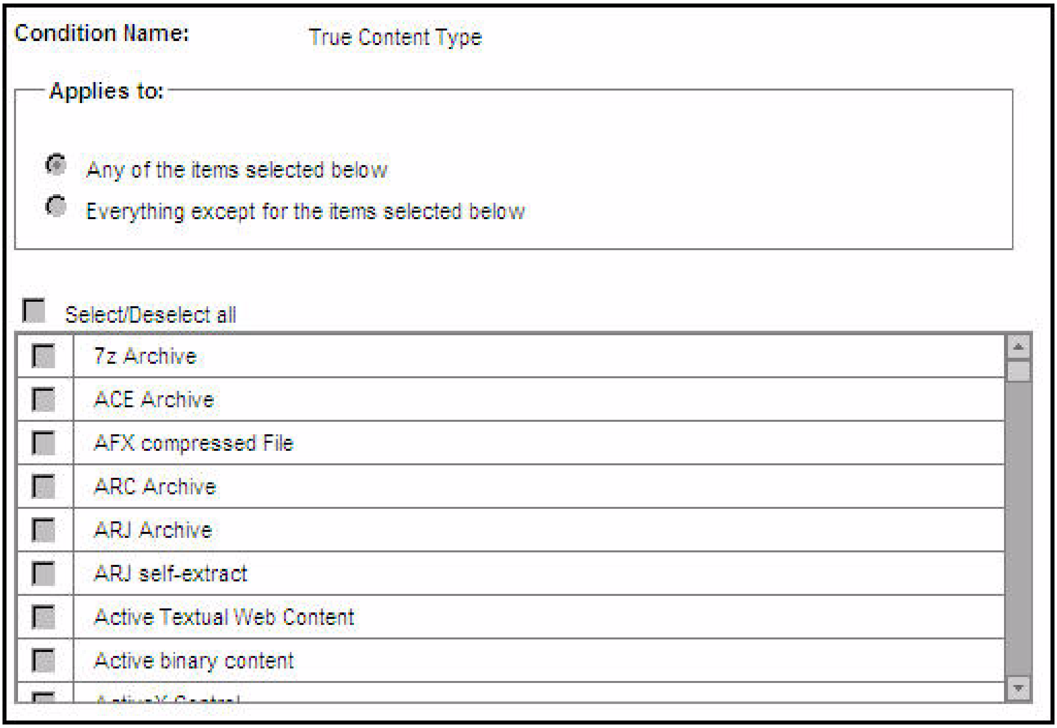
This rule is signed as X-Ray by default. Therefore, logs will indicate that the page would be blocked due to a forbidden operation, and Content blocked due to a suspected data leakage violation.

10.In order to obtain further information about the blocked file click the button under the Request section

The uploaded file is viewable in this screen and the true content type is displayed.

Allow Streaming

The **Allow Streaming** rule was designed in order to allow media streaming (audio, video) to pass through the system.



Condition Name: True Content Type

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

- □ 7z Archive
- □ ACE Archive
- □ AFX compressed File
- □ ARC Archive
- □ ARJ Archive
- □ ARJ self-extract
- □ Active Textual Web Content
- □ Active binary content
- □ ActiveX Control

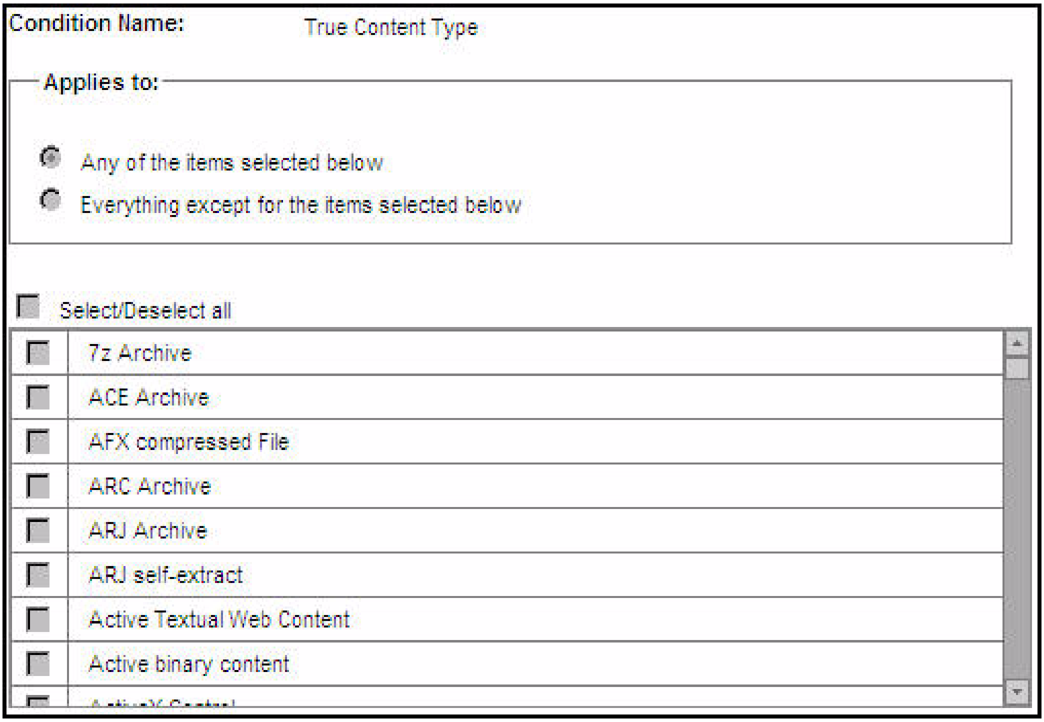
Figure 3-9: Allow Streaming

The following table displays the definitions:

Allow Streaming	
Action	Allow: Bypass Scanning
Conditions	
True Content Type	Streaming

Allow and Scan Customer-Defined True Content Type

This rule allows allows files of a certain true type as defined by system administrators. These files are only subjected so scanning if they are within archive containers. This rule is only relevant if you have chosen categories through the Simplified Setup interface.



Condition Name: True Content Type

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□ 7z Archive

□ ACE Archive

□ AFX compressed File

□ ARC Archive

□ ARJ Archive

□ ARJ self-extract

□ Active Textual Web Content

□ Active binary content

□ ActiveX Control

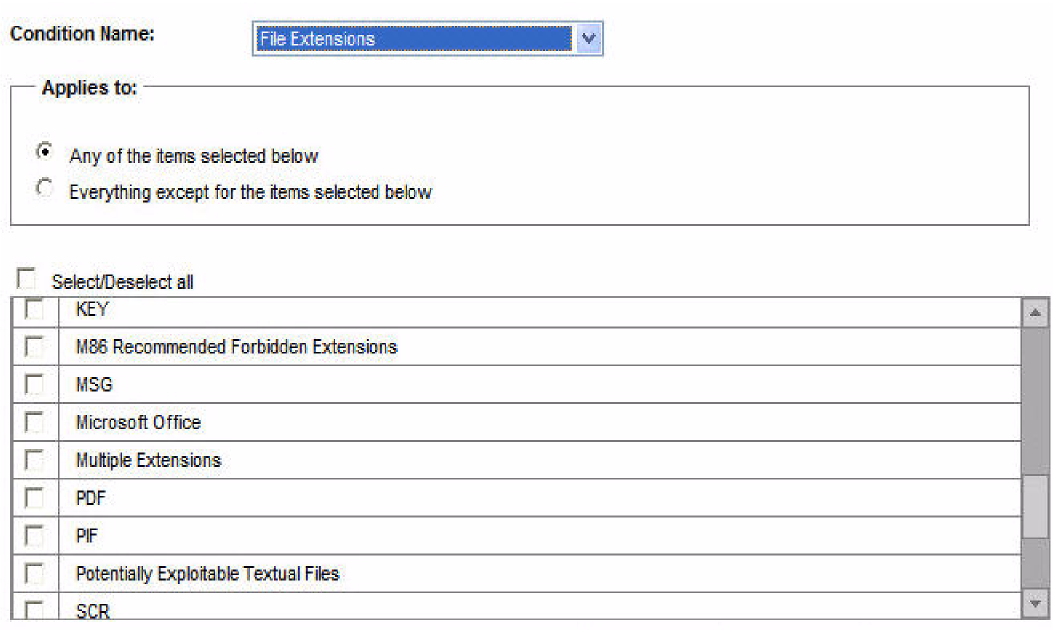
Figure 3-10: Allow and Scan Customer-Defined True Content Type

The following table displays the definitions:

Allow and Scan Customer-Defined True Content Type	
Action	Allow content and scan containers
Conditions	
True Content Type	The categories that you choose in the Simplified Interface will be displayed here.

Allow and Scan Customer-Defined File Extensions

The **Allow and Scan Customer-Defined File Extensions** allows through files with specific extensions whilst scanning files that are containers for potential viruses. This File Extensions Condition Component is different for the three Security Policies: Basic, Medium and Strict.



Condition Name: File Extensions

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

- □ KEY
- □ M86 Recommended Forbidden Extensions
- □ MSG
- □ Microsoft Office
- □ Multiple Extensions
- □ PDF
- □ PIF
- □ Potentially Exploitable Textual Files
- □ SCR

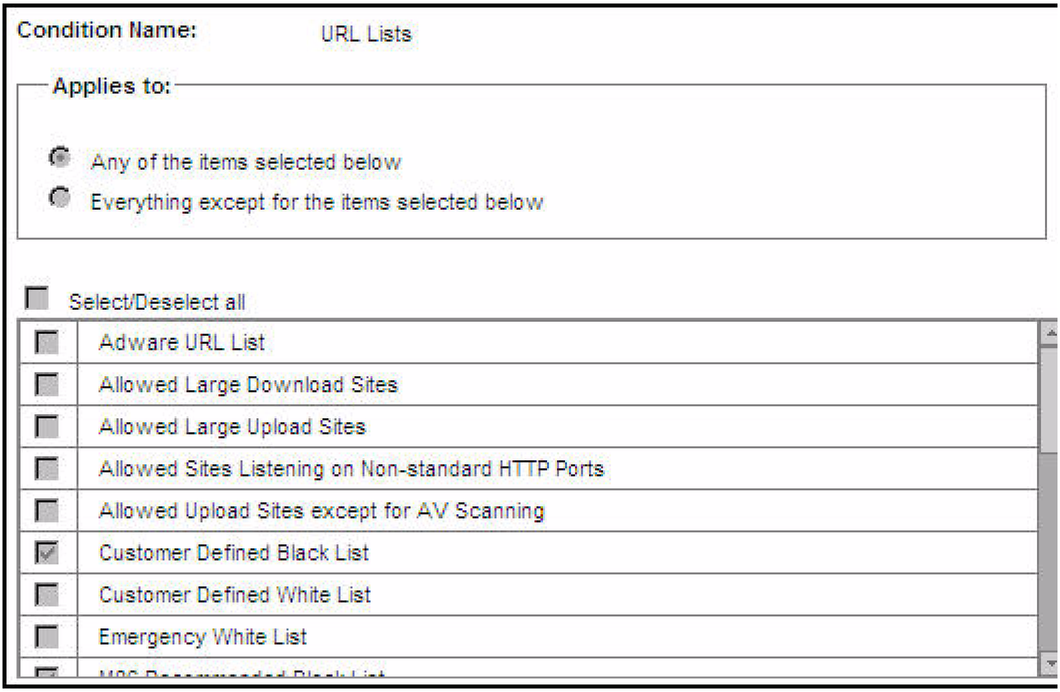
Figure 3-11: Allow and Scan Customer-Defined File Extensions

The following table displays the definitions:

Allow and Scan Customer-Defined File Extensions	
Action	Allow content and scan containers
Conditions	
File Extensions	File Extensions White List (Basic/Medium/ Strict). This list can be edited both through the Simplified Setup and Policies → Condition Settings.

Block Access to Blacklisted Sites

The **Block Access to Blacklisted Sites** rule refers to blocking a list of predefined URLs.



Condition Name: URL Lists

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

- □ Adware URL List
- □ Allowed Large Download Sites
- □ Allowed Large Upload Sites
- □ Allowed Sites Listening on Non-standard HTTP Ports
- □ Allowed Upload Sites except for AV Scanning
- ☑ Customer Defined Black List
- □ Customer Defined White List
- □ Emergency White List
- □ M86 Recommended Black List

Figure 3-12: Block Access to Blacklisted Sites

The following table displays the Rule Editor definitions:

Block Access to Blacklisted Sites	
Action	Block
End-User Message	Blacklisted URL

Block Access to Blacklisted Sites	
Conditions	
URL Lists	Customer Defined Black List, M86 Recommended Black List, URL Black List (Strict/Medium/Basic)

Further Information:

- The **Customer Defined Black List** is a user-defined list of restricted sites. It is accessible via **Lists → URL Lists → Customer Defined Black List**. You can add or delete entries tt this list which will be blocked by SWG.
- The **M86 Recommended Black List c**annot be edited or viewed by the administrator.
- The **Block Access to Blacklisted Sites** rule will be enforced, when its conditions are met, at the request phase.

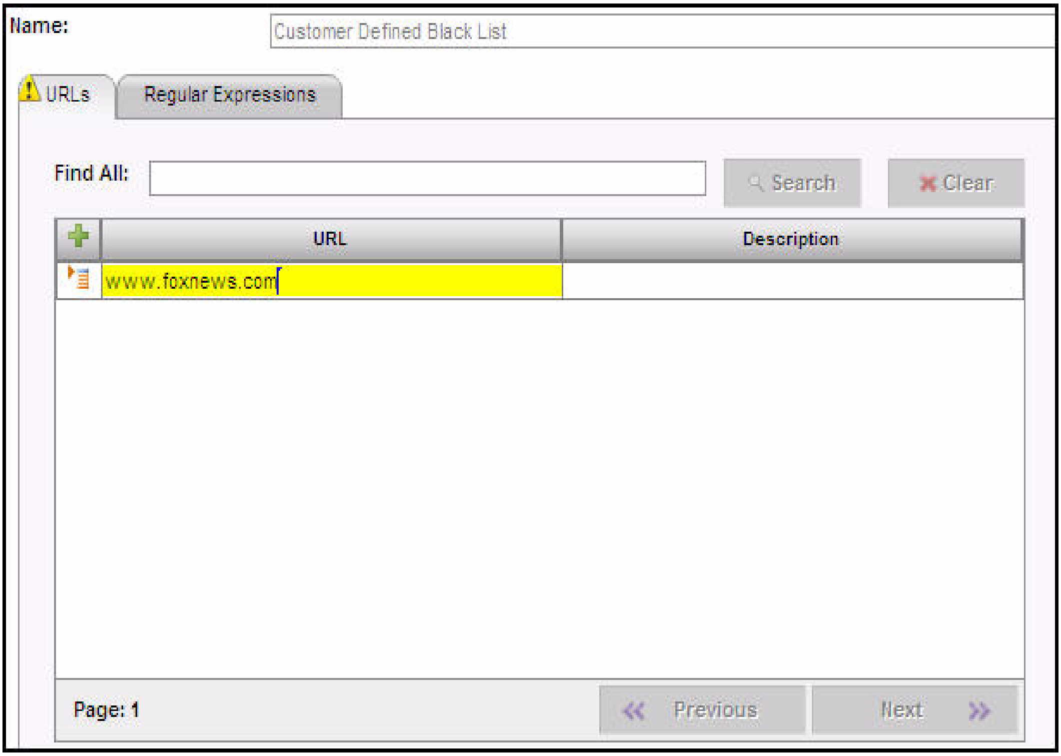
Rule Demonstration:

➲ **To test the Block Access to Blacklisted Sites rule:**

1. Open the Customer Defined Black List by navigating to **Policies → Condition Settings → URL Lists →Customer Defined Black List**.

2. Click **Edit** in the right pane. Next, click on ➕ to add a row.

3. Enter www.cnn.com/* (‘*’ is the wild card, meaning that all URLs contained within www.cnn.com will be blocked).



Name: Customer Defined Black List

URL	Description
www.foxnews.com	

Page: 1

Figure 3-13: Add Item-URL List

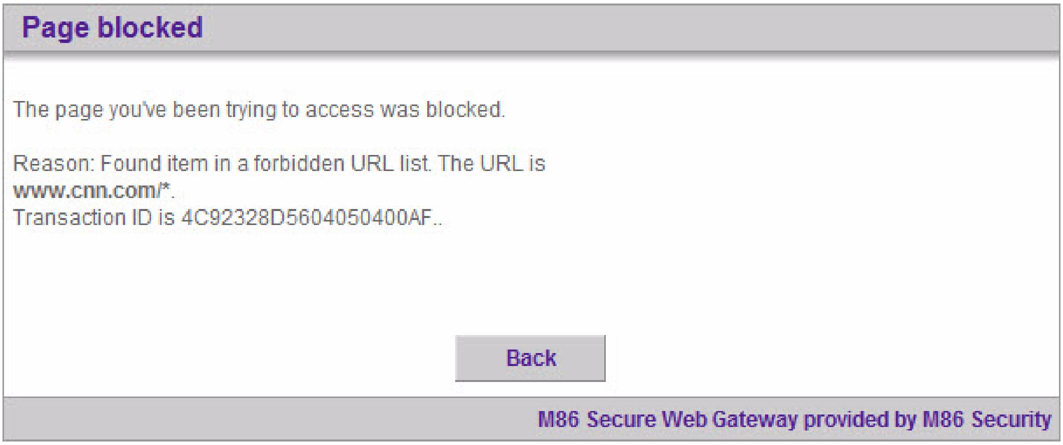
4. Click **Save**. The entry: www.cnn.com/* now appears in the **Customer Defined Black List**.

5. Next, click .

➲ **To test that this website was blocked:**

1. Copy and paste www.cnn.com into your browser:

The following message should appear:



Page blocked

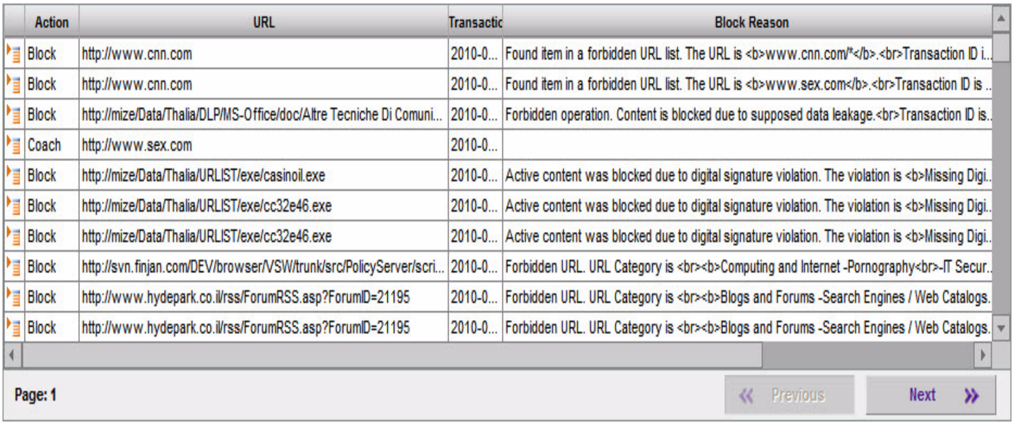
The page you've been trying to access was blocked.

Reason: Found item in a forbidden URL list. The URL is **www.cnn.com/***.
Transaction ID is 4C92328D5604050400AF..

Figure 3-14: Page Blocked Message – Blacklisted Sites

NOTES: *The transaction ID refers to the unique interaction between the end-user and the SWG system*

2. Return to the Management Console and select **Logs & Reports → View Web Logs** menu in the Main Navigation bar.



	Action	URL	Transactic	Block Reason
	Block	http://www.cnn.com	2010-0...	Found item in a forbidden URL list. The URL is <b>www.cnn.com/*</b>. Transaction ID i...
	Block	http://www.cnn.com	2010-0...	Found item in a forbidden URL list. The URL is <b>www.sex.com</b>. Transaction ID is ..
	Block	http://mize/Data/Thalia/DLP/MS-Office/doc/Altre Tecniche Di Comuni...	2010-0...	Forbidden operation. Content is blocked due to supposed data leakage. Transaction ID is..
	Coach	http://www.sex.com	2010-0...	
	Block	http://mize/Data/Thalia/URLIST/exe/casinoil.exe	2010-0...	Active content was blocked due to digital signature violation. The violation is <b>Missing Digi..
	Block	http://mize/Data/Thalia/URLIST/exe/cc32e46.exe	2010-0...	Active content was blocked due to digital signature violation. The violation is <b>Missing Digi..
	Block	http://mize/Data/Thalia/URLIST/exe/cc32e46.exe	2010-0...	Active content was blocked due to digital signature violation. The violation is <b>Missing Digi..
	Block	http://svn.finjan.com/DEV/browser/VSW/trunk/src/PolicyServer/scri...	2010-0...	Forbidden URL. URL Category is <b>Computing and Internet -Pornography -IT Secur..
	Block	http://www.hydepark.co.il/rss/ForumRSS.asp?ForumID=21195	2010-0...	Forbidden URL. URL Category is <b>Blogs and Forums -Search Engines / Web Catalogs.
	Block	http://www.hydepark.co.il/rss/ForumRSS.asp?ForumID=21195	2010-0...	Forbidden URL. URL Category is <b>Blogs and Forums -Search Engines / Web Catalogs.

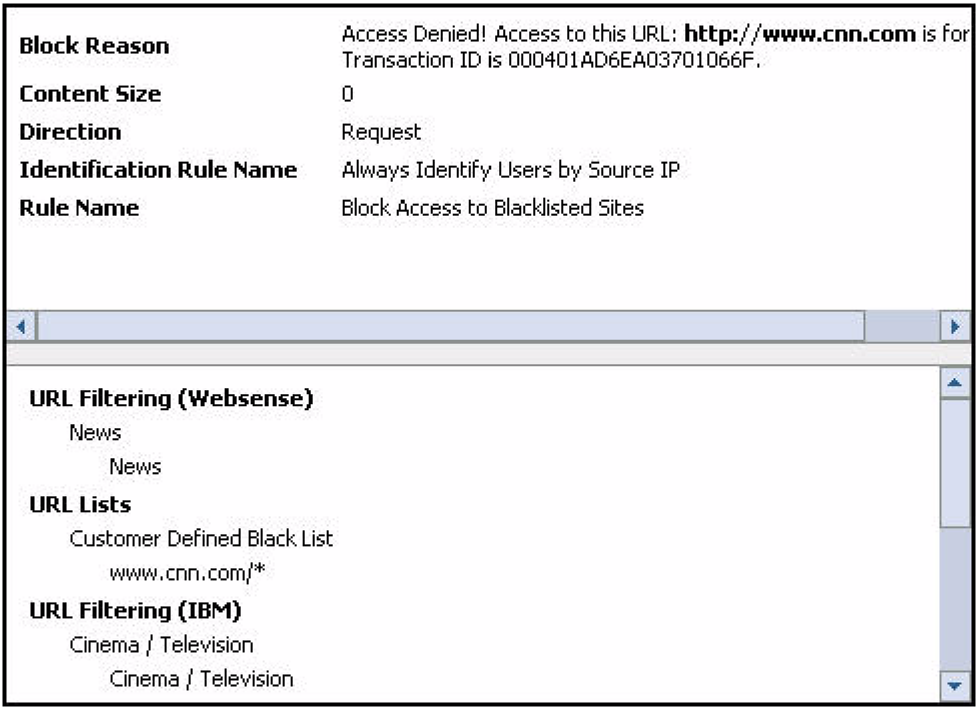
Page: 1

Figure 3-15: Web Logs

3. In the same row as the blocked **cnn.com** transaction, click and select Details. The Transaction Detail tabs include

Transaction, User, Policy Enforcement, Content and Scanning Server details.

4. In the Transaction Details tree, click **Request** to obtain further information on the Request phase of this transaction. Only the Request component exists for this transaction since it was blocked at the request phase.



Block Reason	Access Denied! Access to this URL: **http://www.cnn.com** is for Transaction ID is 000401AD6EA03701066F.
Content Size	0
Direction	Request
Identification Rule Name	Always Identify Users by Source IP
Rule Name	Block Access to Blacklisted Sites

URL Filtering (Websense)

News

News

URL Lists

Customer Defined Black List

www.cnn.com/*

URL Filtering (IBM)

Cinema / Television

Cinema / Television

Figure 3-16: Request: Blacklisted Site

➲ **To remove this website from the Customer Defined Black List:**

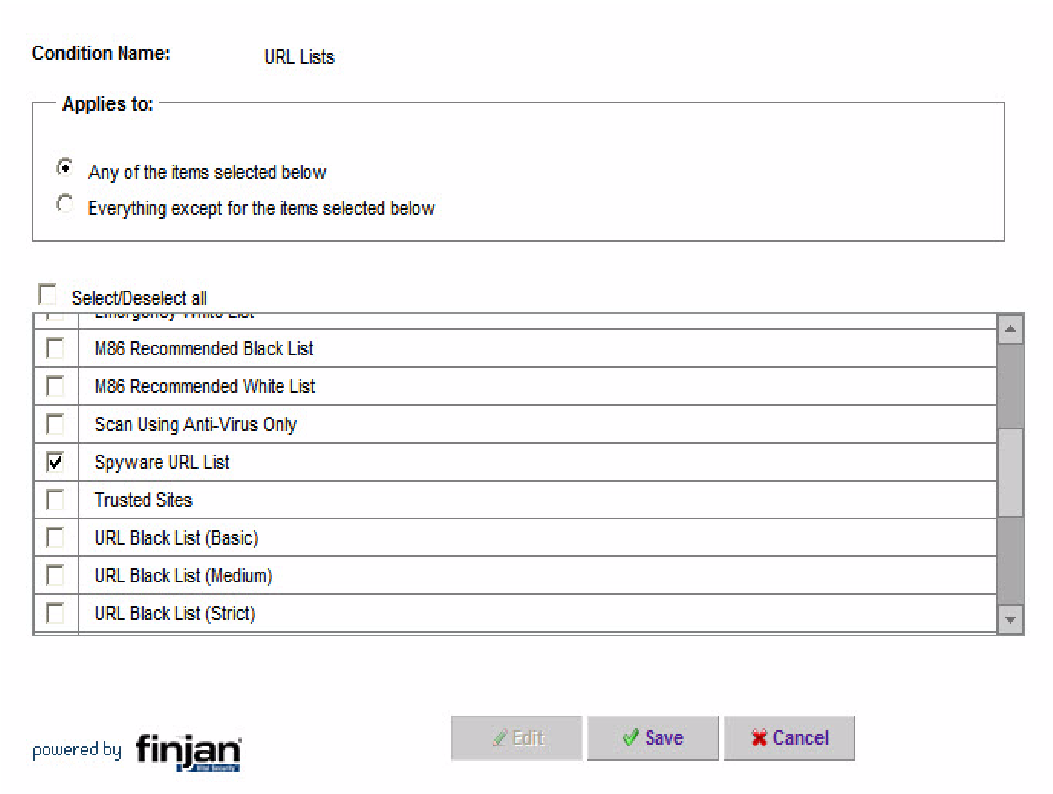
1. Navigate to the list via **Policies → Condition Settings → URL Lists →Customer Defined Black List**.
2. Click **Edit** to open the screen for editing.

3. Click to the left of **www.cnn.com**, and select **Delete** in the right pane.

4. Click **Save** and then click .

Block Access to Spyware Sites

The **Block Access to Spyware Sites** rule refers to blocking predefined Spyware Sites.



Condition Name: URL Lists

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

□	Emergency White List
□	M86 Recommended Black List
□	M86 Recommended White List
□	Scan Using Anti-Virus Only
☑	Spyware URL List
□	Trusted Sites
□	URL Black List (Basic)
□	URL Black List (Medium)
□	URL Black List (Strict)

Figure 3-17: Block Access to Spyware Sites

The following table displays the definitions:

Block Access to Spyware Sites	
Action	Block
End-User Message	Blocked Spyware URL
Conditions	
URL Lists	Spyware URL List

Further Information:

- The **Block Access to Spyware Sites** rule will be enforced, if its conditions were met, at the request phase.
- The Spyware URL List is generated by M86 and is not accessible by the administrator.

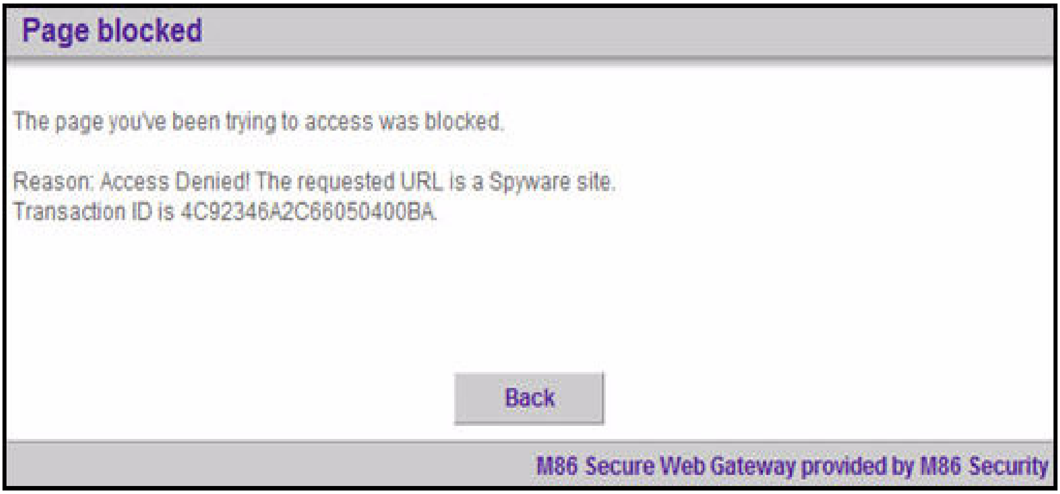
Rule Demonstration:

➲ **To test the Block Access to Spyware Sites rule:**

1. Copy and paste the following URLs (known spyware sites into your browser):

   www.dplog.com
   www.search-world.net
   www.cashsearch.biz

The following message should appear when trying to access any of the above pages.



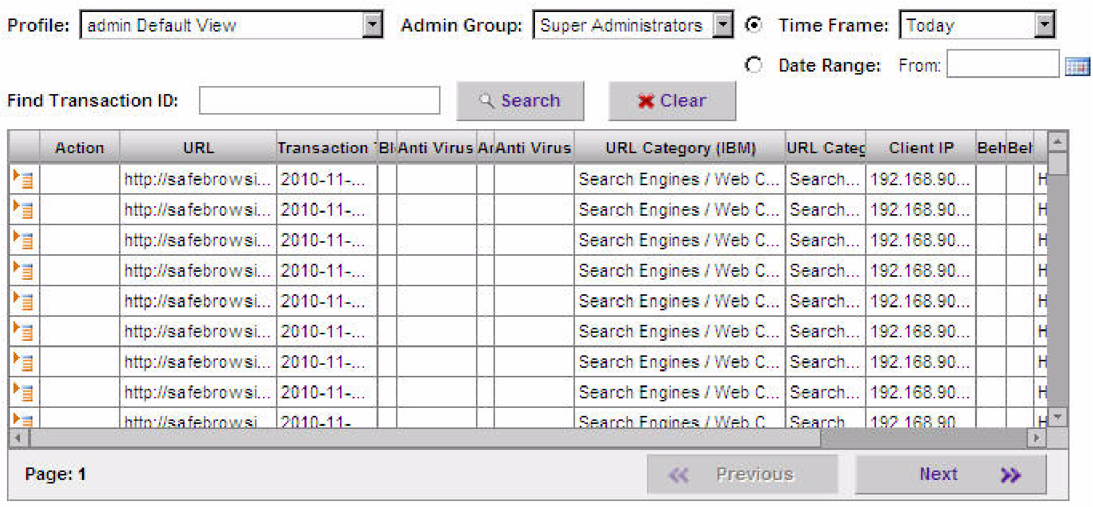
Page blocked

The page you've been trying to access was blocked.

Reason: Access Denied! The requested URL is a Spyware site.
Transaction ID is 4C92346A2C66050400BA.

Figure 3-18: Page Blocked Message – Spyware Sites

2. Return to the Management Console and select the **Logs** → **View Web Logs** menu in the Main Navigation bar.



Profile: admin Default View   Admin Group: Super Administrators   ● Time Frame: Today

○ Date Range: From:

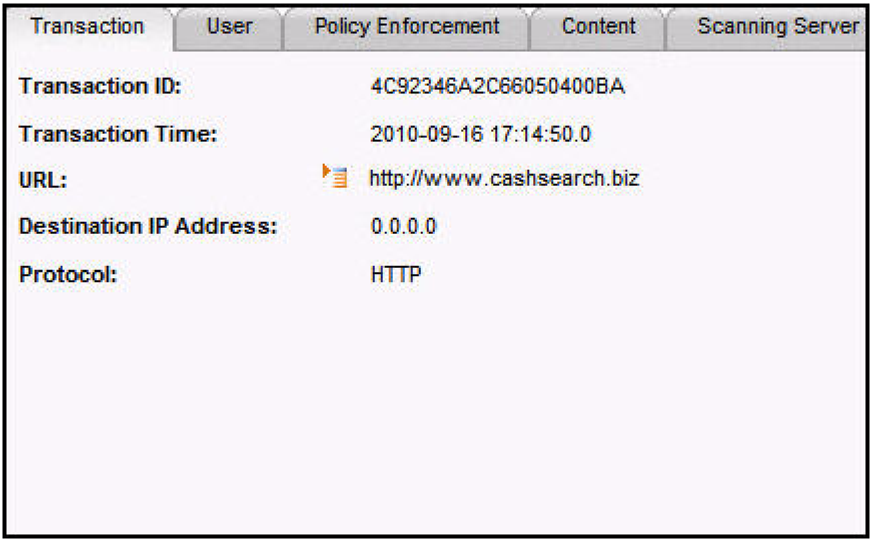
Find Transaction ID:

	Action	URL	Transaction I	Bl	Anti Virus	Ar	Anti Virus	URL Category (IBM)	URL Categ	Client IP	Beh	Bel	
▸		http://safebrowsi...	2010-11-...					Search Engines / Web C...	Search...	192.168.90...			H
▸		http://safebrowsi...	2010-11-...					Search Engines / Web C...	Search...	192.168.90...			H
▸		http://safebrowsi...	2010-11-...					Search Engines / Web C...	Search...	192.168.90...			H
▸		http://safebrowsi...	2010-11-...					Search Engines / Web C...	Search...	192.168.90...			H
▸		http://safebrowsi...	2010-11-...					Search Engines / Web C...	Search...	192.168.90...			H
▸		http://safebrowsi...	2010-11-...					Search Engines / Web C...	Search...	192.168.90...			H
▸		http://safebrowsi...	2010-11-...					Search Engines / Web C...	Search...	192.168.90...			H
▸		http://safebrowsi...	2010-11-...					Search Engines / Web C...	Search...	192.168.90...			H
▸		http://safebrowsi	2010-11-					Search Engines / Web C	Search	192.168.90			H

Page: 1

Figure 3-19: View Web Logs

3. In the same row as the blocked transaction, click and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.



Transaction ID: 4C92346A2C66050400BA

Transaction Time: 2010-09-16 17:14:50.0

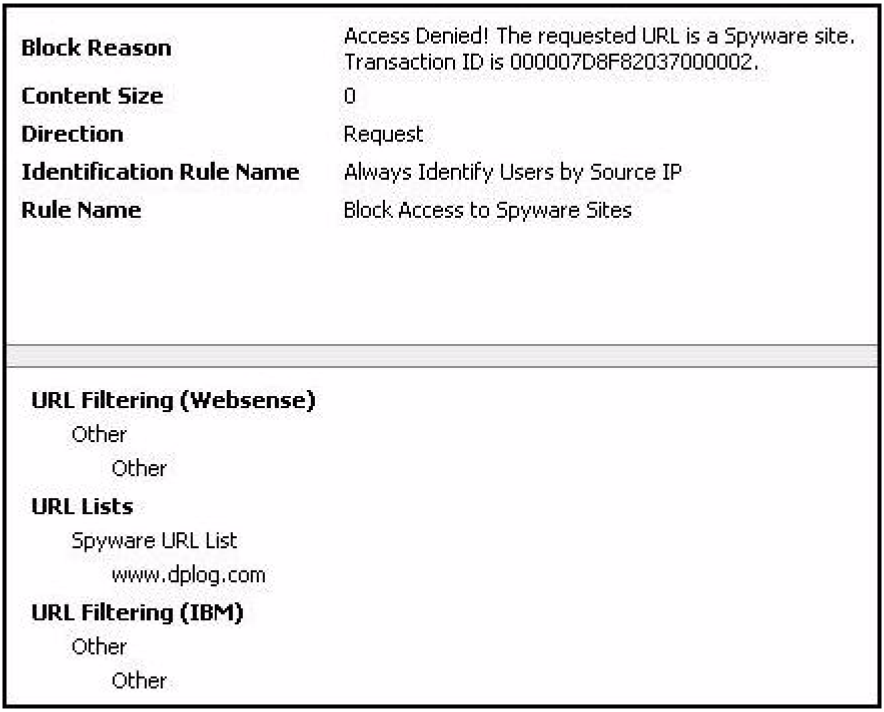
URL: http://www.cashsearch.biz

Destination IP Address: 0.0.0.0

Protocol: HTTP

Figure 3-20: Transaction Details - Spyware Site

4. In the Transaction Details tree, click **Request** to obtain further information on the Request phase of this transaction. Only the Request component exists for this transaction since it was blocked at the request phase.



Block Reason	Access Denied! The requested URL is a Spyware site. Transaction ID is 000007D8F82037000002.
Content Size	0
Direction	Request
Identification Rule Name	Always Identify Users by Source IP
Rule Name	Block Access to Spyware Sites

URL Filtering (Websense)
- Other
  - Other

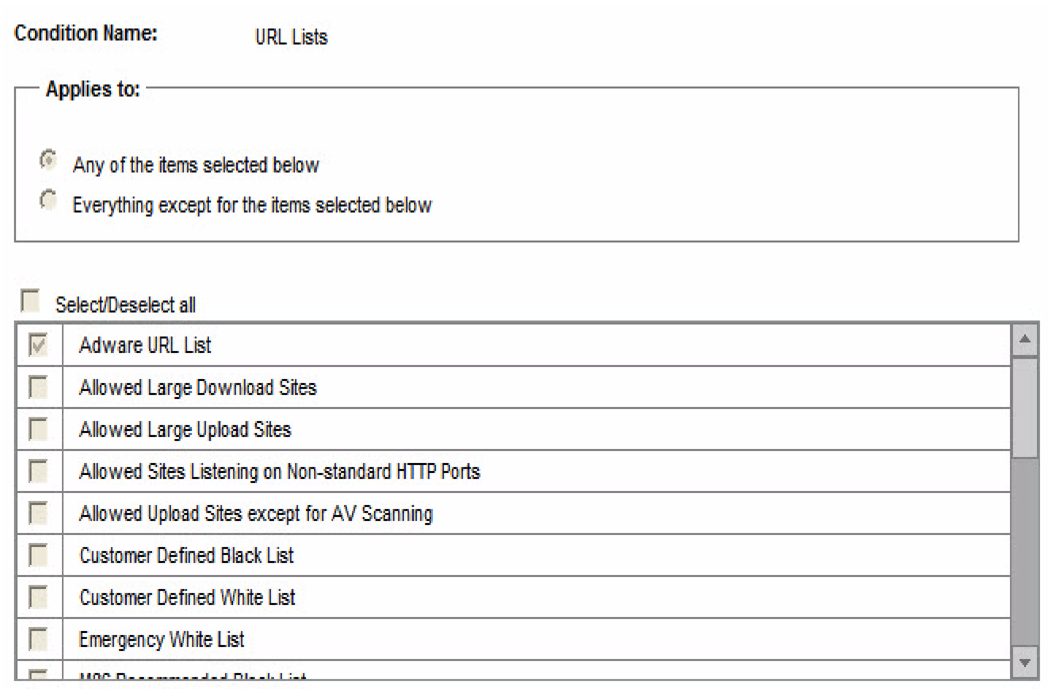
URL Lists
- Spyware URL List
  - www.dplog.com

URL Filtering (IBM)
- Other
  - Other

Figure 3-21: Request: Spyware Sites

Block Access to Adware Sites

The **Block Access to Adware Sites** rule refers to blocking predefined Adware Sites.



Condition Name: URL Lists

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

☑ Adware URL List

□ Allowed Large Download Sites

□ Allowed Large Upload Sites

□ Allowed Sites Listening on Non-standard HTTP Ports

□ Allowed Upload Sites except for AV Scanning

□ Customer Defined Black List

□ Customer Defined White List

□ Emergency White List

□ M86 Recommended Black List

Figure 3-22: Block Access to Adware Sites

The following table displays the definitions:

Block Access to Adware Sites	
Action	Block
End-User Message	Blocked Adware URL
Conditions	
URL Lists	Adware URL List

Further Information:

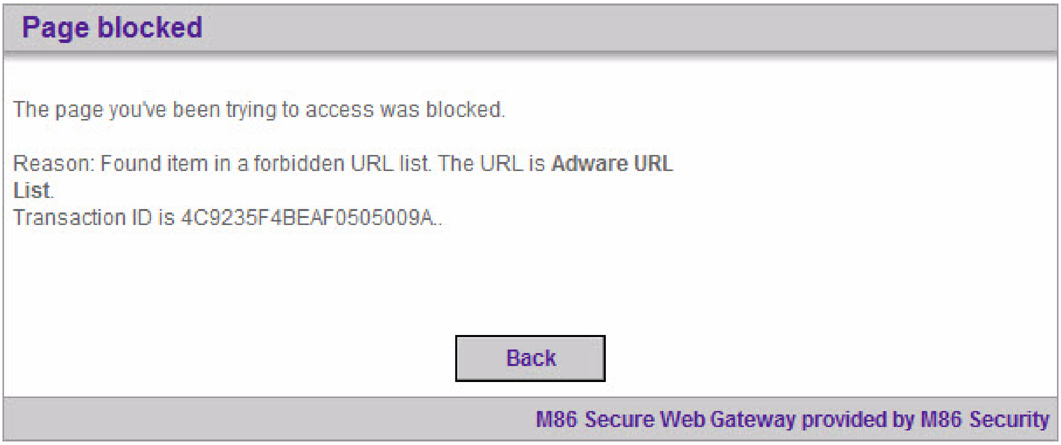
- The **Block Access to Adware Sites** rule will be enforced, if its conditions were met, at the request phase.
- The Adware URL List is generated by M86 and is not accessible by the administrator.

Rule Demonstration:

➲ **To test the Block Access to Adware Sites rule:**

1. Copy and paste the following URL into your browser (known adware): www.infinityads.com

The following message should appear when trying to access this site.



Page blocked

The page you've been trying to access was blocked.

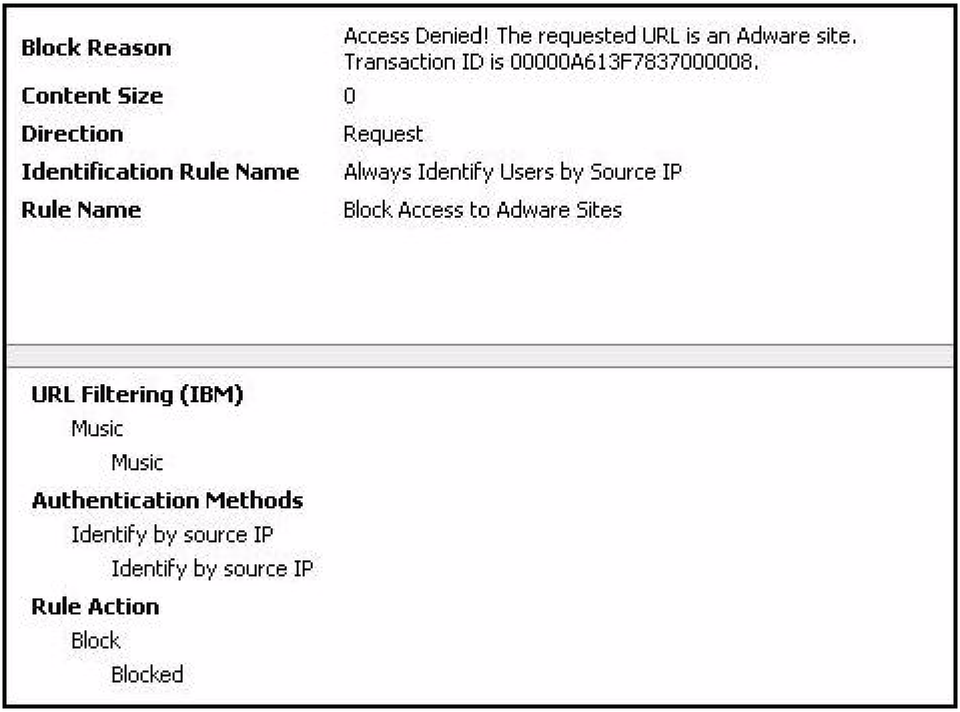
Reason: Found item in a forbidden URL list. The URL is **Adware URL List**.
Transaction ID is 4C9235F4BEAF0505009A..

Figure 3-23: Page Blocked Message – Adware Sites

2. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
3. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction,

User, Policy Enforcement, Content and Scanning Server details.

4. In the Transaction Details tree, click **Request** to obtain further information on the Request phase of this transaction. Only the Request component exists for this transaction since it was blocked at the request phase.



Block Reason	Access Denied! The requested URL is an Adware site. Transaction ID is 00000A613F7837000008.
Content Size	0
Direction	Request
Identification Rule Name	Always Identify Users by Source IP
Rule Name	Block Access to Adware Sites

URL Filtering (IBM)
- Music
  - Music

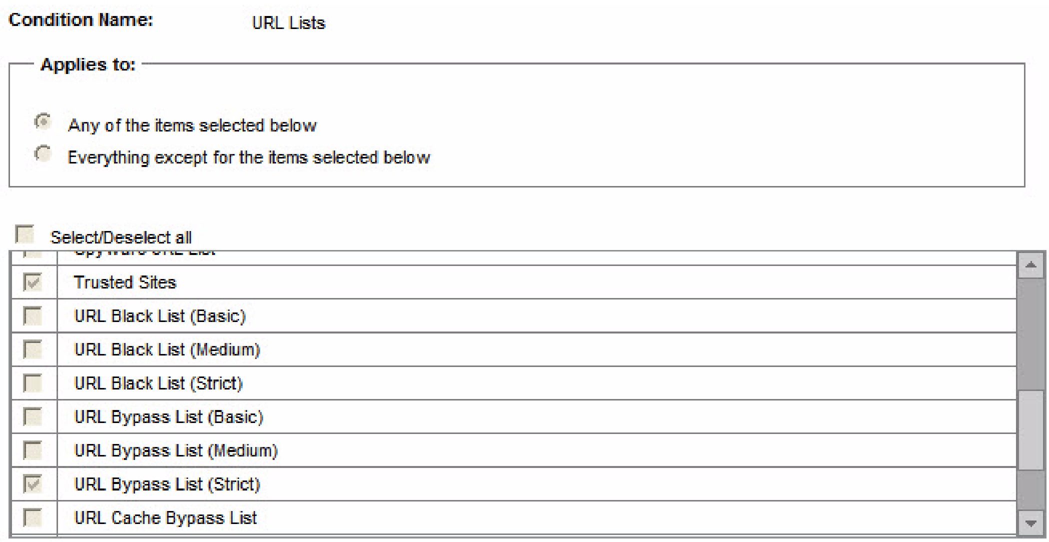
Authentication Methods
- Identify by source IP
  - Identify by source IP

Rule Action
- Block
  - Blocked

Figure 3-24: Request: Adware Sites

Allow Trusted Sites

The **Allow Trusted Sites** rule refers to Security scanning being disabled completely on highly trusted sites (as long as they are not blacklisted or part of a Spyware/Adware list).



Condition Name: URL Lists

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□	Spyware URL List
☑	Trusted Sites
□	URL Black List (Basic)
□	URL Black List (Medium)
□	URL Black List (Strict)
□	URL Bypass List (Basic)
□	URL Bypass List (Medium)
☑	URL Bypass List (Strict)
□	URL Cache Bypass List

Figure 3-25: Allow Trusted Sites

The following table displays the definitions:

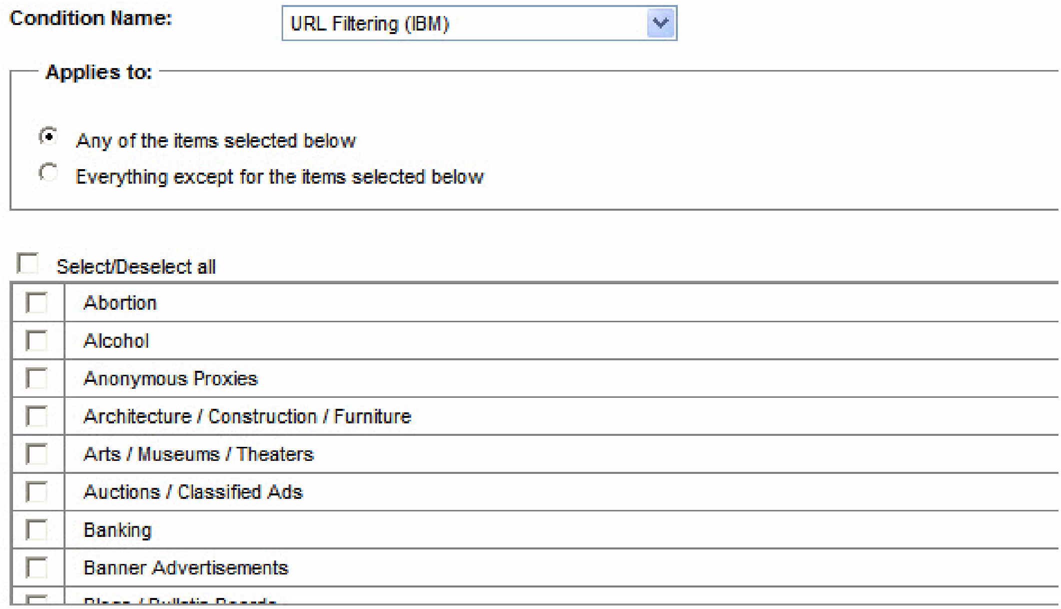
Allow Trusted Sites	
Action	Bypass Scanning
Conditions	
URL Lists	Trusted Sites, Allow Large Download Sites, URL Bypass List (Basic/Medium/Strict)

Further Information:

- As this rule is run prior to other security rules (apart from blacklisted or spyware/adware sites), all the sites within the Trusted Sites and URL Bypass List will not be scanned for any security breach. Therefore, M86 recommends only using these for selected sites and using the regular Customer Defined White List for the majority of trusted sites.

Customer-Defined URL Filtering (Websense/ IBM)

The **Customer-Defined URL Filtering** rule refers to blocking a list of URL categories - either from Websense or IBM Proventia Web Filter - depending on your license. This rule is only relevant if you have selected categories through the Simplified Policies interface.



Condition Name: URL Filtering (IBM)

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

- □ Abortion
- □ Alcohol
- □ Anonymous Proxies
- □ Architecture / Construction / Furniture
- □ Arts / Museums / Theaters
- □ Auctions / Classified Ads
- □ Banking
- □ Banner Advertisements

Figure 3-26: Customer-Defined URL Filtering

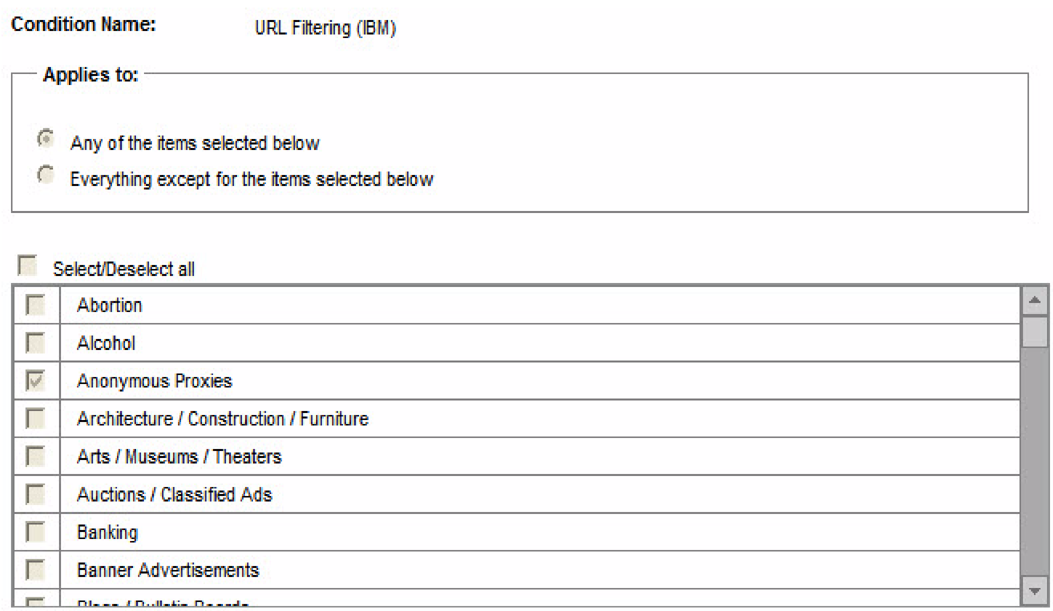
The following table displays the definitions:

Customer-Defined URL Filtering	
Action	Block
End-User Message	Blocked URL Category

Customer-Defined URL Filtering	
Conditions	
Customer-Defined URL Filtering (Websense/IBM)	The categories that you choose in the Simplified Setup URL Categorization block will be displayed here.

Block Access to High-Risk Site Categories (Websense/IBM)

The Block Access to High-Risk Site Categories rule refers to blocking a list of predefined URL categories - either from Websense or IBM Proventia Web Filter - depending on your license.



Condition Name: URL Filtering (IBM)

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

- □ Abortion
- □ Alcohol
- ☑ Anonymous Proxies
- □ Architecture / Construction / Furniture
- □ Arts / Museums / Theaters
- □ Auctions / Classified Ads
- □ Banking
- □ Banner Advertisements
- □ Blogs / Bulletin Boards

Figure 3-27: Block Access to High-Risk Site Categories

The following table displays the definitions:

Block Access to High-Risk Site Categories	
Action	Block
End-User Message	Blocked URL Category
Conditions	
URL Filtering (Websense)	Adult/Sexually Explicit, Hacking, Proxies and Translators
URL Filtering (IBM)	Anonymous Proxies, Computer Crime, Erotic/ Sex, Malware, Phishing URLs, Pornography, Spam URLs, Warez/Hacking/Illegal Software

Further Information:

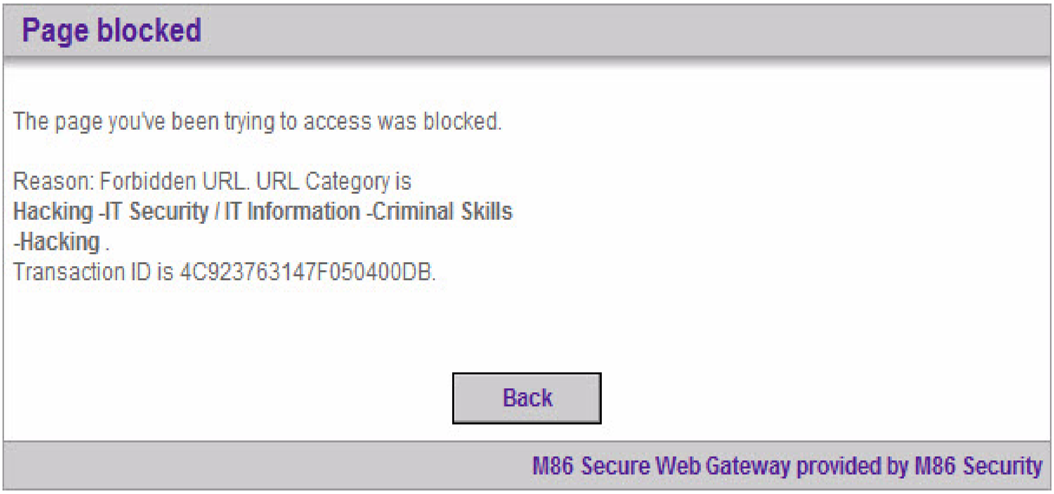
- The **Block Access to High-Risk Sites Categories** rule will be enforced, if its conditions were met, at the request phase.
- Websense and IBM Provenia Web Filter engines require a license.

Rule Demonstration:

➲ **To test the Block Access to High-Risk Site Categories rule:**

1. Copy and paste the following URL into your browser**:**

   http://www.hackingexposed.com/. The following error message is displayed.

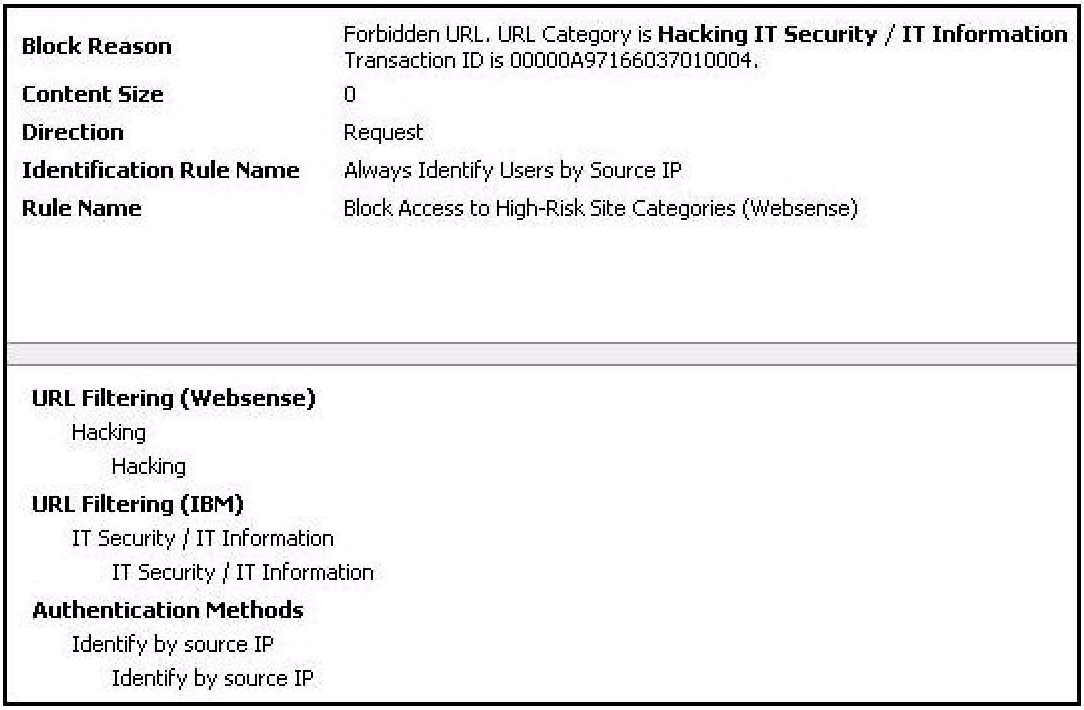

Page blocked

The page you've been trying to access was blocked.

Reason: Forbidden URL. URL Category is
Hacking -IT Security / IT Information -Criminal Skills -Hacking .
Transaction ID is 4C923763147F050400DB.

Figure 3-28: Page Blocked Message- Hacking

2. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
3. In the same row as the blocked transaction, click and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
4. In the Transaction Details tree, click **Request** to obtain further information on the Request phase of this transaction. Only the Request component exists for this transaction since it was blocked at the request phase..



Block Reason	Forbidden URL. URL Category is **Hacking IT Security / IT Information** Transaction ID is 00000A97166037010004.
Content Size	0
Direction	Request
Identification Rule Name	Always Identify Users by Source IP
Rule Name	Block Access to High-Risk Site Categories (Websense)

URL Filtering (Websense)
- Hacking
  - Hacking

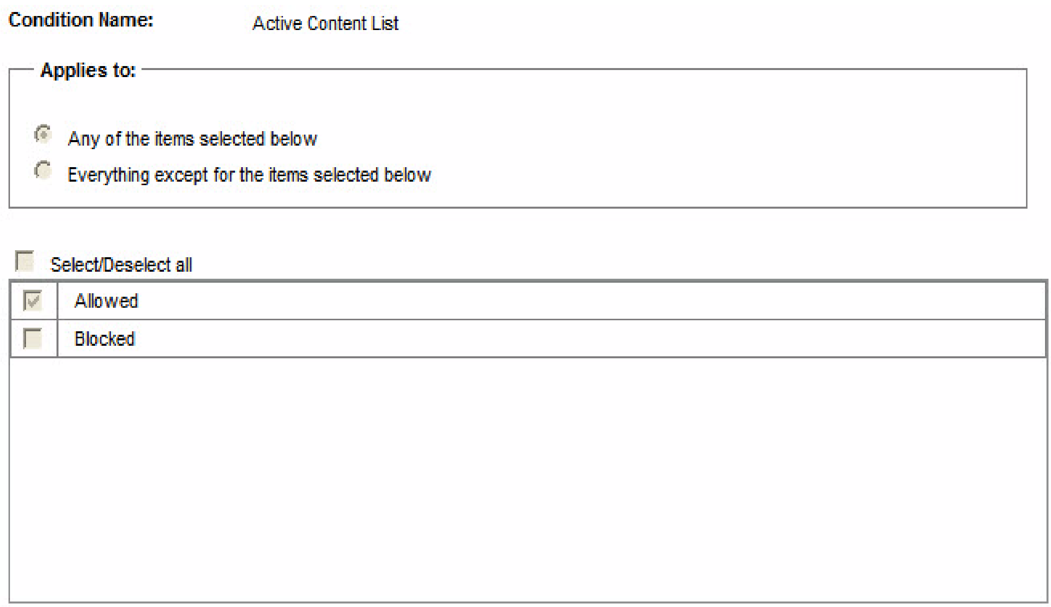
URL Filtering (IBM)
- IT Security / IT Information
  - IT Security / IT Information

Authentication Methods
- Identify by source IP
  - Identify by source IP

Figure 3-29: Request: High-Risk Site Categories - Hacking

Allow Whitelisted ActiveX, Java Applets and Executables

The **Allow Whitelisted ActiveX, Java Applets** and **Executables** rule will allow those items which were moved to the “Allowed” Active Content List.



Condition Name: Active Content List

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

☑	Allowed
□	Blocked

Figure 3-30: Allow Whitelisted ActiveX, Java Applets and Executables

The following table displays the definitions:

Allow Whitelisted ActiveX, Java Applets and Executables	
Action	Allow
Conditions	
Active Content List	Allowed

Further Information:

- SWG creates signatures for active content (Java Applets, ActiveX and Executable files) that passes through it. These signatures are available in the Active Content List (navigate to **Policies →Condition Settings → Active Content List →Auto-generated**).
- From the **Auto-generated list** you can move an entry to a destination group (i.e. Allowed list and Blocked list). For the

Default M86 Security Policy, once you move an entry to the Allowed list, next time a client requests the Allowed entry, the content will be passed without scanning (based on signature only). This enables the administrator to specifically allow binary active content.

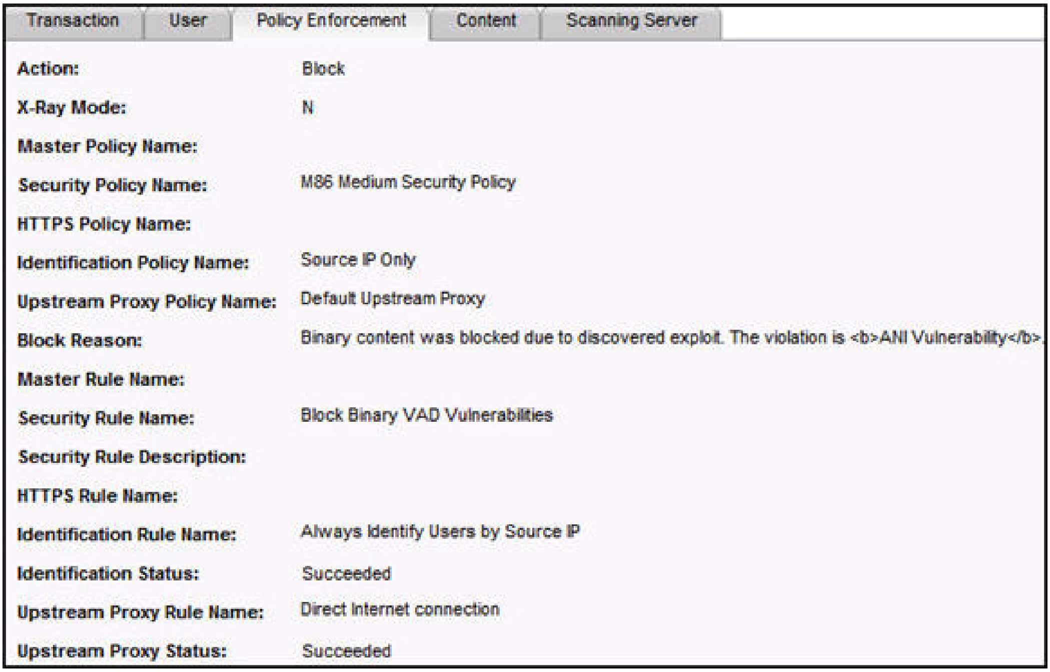
- The **Allow Whitelisted ActiveX, Java Applets and Executables** rule will be enforced, if its conditions were met, at the response phase.

Allow Known Legitimate Content

The **Allow Known Legitimate Content** rule was designed to bypass scanning for a selection of files that have been approved as known legitimate content by M86.

The following table displays the Rule Editor definitions:

Allow Known Legitimate Content	
Action	Allow
End-User Message	Active Content List
Conditions	
Static Content	This condition is used to identify known Malicious Objects based on their malicious behavior signatures.



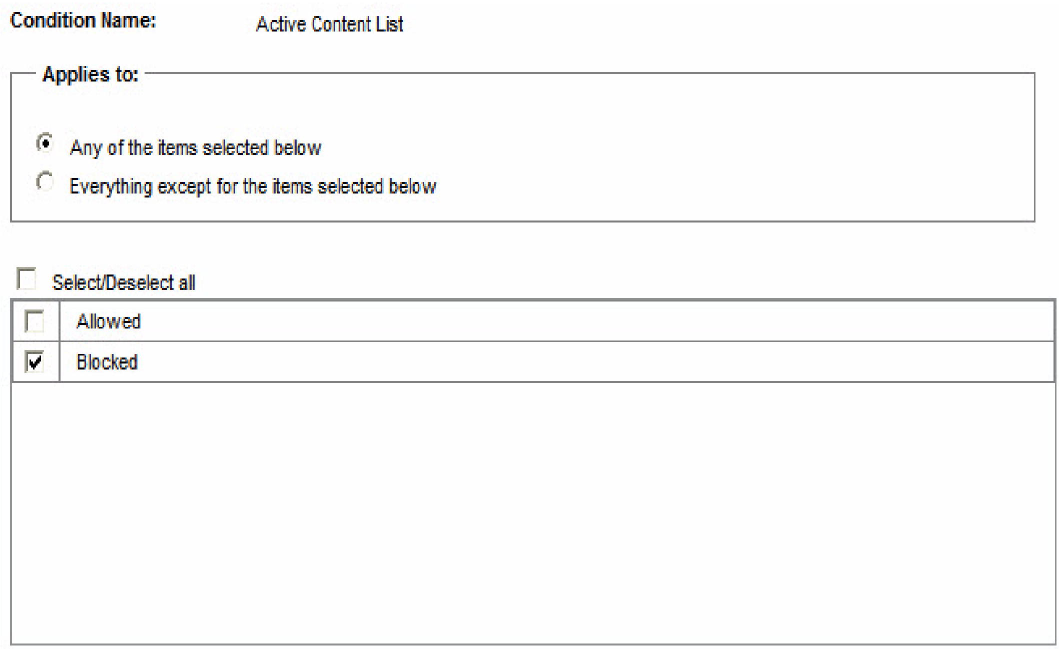
Action:	Block
X-Ray Mode:	N
Master Policy Name:	
Security Policy Name:	M86 Medium Security Policy
HTTPS Policy Name:	
Identification Policy Name:	Source IP Only
Upstream Proxy Policy Name:	Default Upstream Proxy
Block Reason:	Binary content was blocked due to discovered exploit. The violation is <b>ANI Vulnerability</b>
Master Rule Name:	
Security Rule Name:	Block Binary VAD Vulnerabilities
Security Rule Description:	
HTTPS Rule Name:	
Identification Rule Name:	Always Identify Users by Source IP
Identification Status:	Succeeded
Upstream Proxy Rule Name:	Direct Internet connection
Upstream Proxy Status:	Succeeded

Figure 3-31: Allow Legitimate Content Policy Enforcement Details

This page was Allowed due to the Allow Known Legitimate Content rule.

Block ActiveX, Java Applets and Executables by ACL

The **Block ActiveX, Java Applets** and **Executables by ACL** rule will cause the SWG Appliance to block the items which were moved to the “Blocked” Active Content List.



Condition Name: Active Content List

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

□	Allowed
☑	Blocked

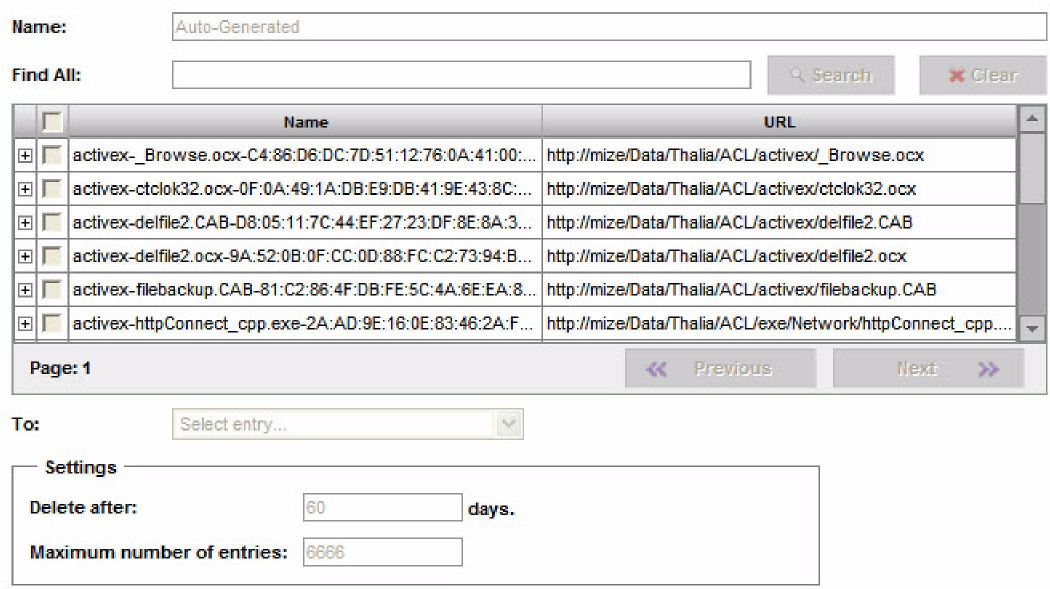
Figure 3-32: Block ActiveX, Java Applets and Executables by ACL

The following table displays the Rule Editor definitions:

Block ActiveX, Java Applets and Executables by ACL	
Action	Block
End-User Message	Active Content List
Conditions	
True Content Type	Active binary content
Active Content List	Blocked

Further Information:

- SWG creates signatures for active content (Java Applets, ActiveX and Executable files) that passes through the system. These signatures are available under the Active Content List, and can be seen via **Policies →Condition Settings → Active Content List →Auto-generated**.



Name: Auto-Generated

Find All:

Search | Clear

	□	Name	URL
⊞	□	activex-_Browse.ocx-C4:86:D6:DC:7D:51:12:76:0A:41:00:...	http://mize/Data/Thalia/ACL/activex/_Browse.ocx
⊞	□	activex-ctclok32.ocx-0F:0A:49:1A:DB:E9:DB:41:9E:43:8C:...	http://mize/Data/Thalia/ACL/activex/ctclok32.ocx
⊞	□	activex-delfile2.CAB-D8:05:11:7C:44:EF:27:23:DF:8E:8A:3...	http://mize/Data/Thalia/ACL/activex/delfile2.CAB
⊞	□	activex-delfile2.ocx-9A:52:0B:0F:CC:0D:88:FC:C2:73:94:B...	http://mize/Data/Thalia/ACL/activex/delfile2.ocx
⊞	□	activex-filebackup.CAB-81:C2:86:4F:DB:FE:5C:4A:6E:EA:8...	http://mize/Data/Thalia/ACL/activex/filebackup.CAB
⊞	□	activex-httpConnect_cpp.exe-2A:AD:9E:16:0E:83:46:2A:F...	http://mize/Data/Thalia/ACL/exe/Network/httpConnect_cpp....

Page: 1

<< Previous | Next >>

To: Select entry...

Settings

Delete after: 60 days.

Maximum number of entries: 6666

Figure 3-33: Auto-generated Screen

- From the Auto-generated screen, you can move an entry to a destination group (i.e. Allowed list and Blocked list). Once you have moved an entry to the Blocked list, the next time an end-user requests a blacklisted entry, the content will be blocked automatically (without scanning) – based on signature only.
- The **Block ActiveX, Java Applets and Executables by ACL** rule will be enforced, if its conditions were met, at the Response phase (unless it is uploaded).

Rule Demonstration:

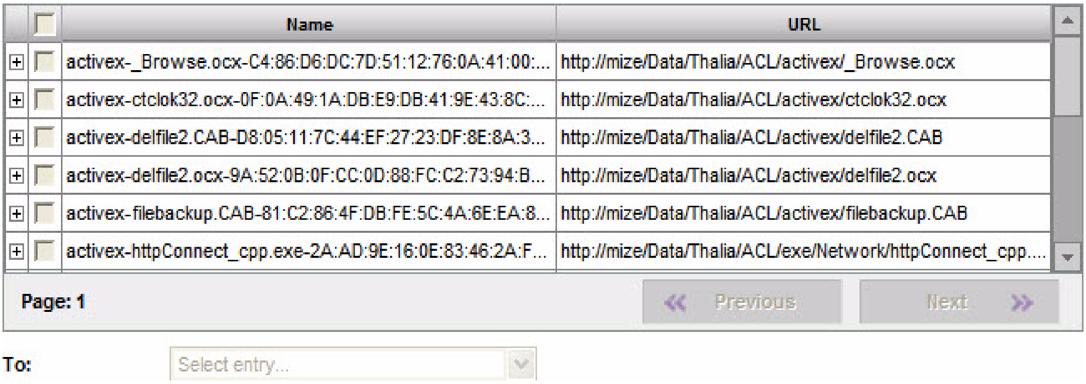
➲ **To test the Block ActiveX, Java Applets and Executables by ACL rule:**

1. Go to a site that uses Java Applets such as:

http://java.sun.com/applets/jdk/1.3/

2. click on one of the examples to the left, for example: Dither Test.

3. Navigate to **Policies →Condition Settings→Active Content List →Auto-generated** to open the Auto-generated screen showing active content.



	□	Name	URL
⊞	□	activex-_Browse.ocx-C4:86:D6:DC:7D:51:12:76:0A:41:00:...	http://mize/Data/Thalia/ACL/activex/_Browse.ocx
⊞	□	activex-ctclok32.ocx-0F:0A:49:1A:DB:E9:DB:41:9E:43:8C:...	http://mize/Data/Thalia/ACL/activex/ctclok32.ocx
⊞	□	activex-delfile2.CAB-D8:05:11:7C:44:EF:27:23:DF:8E:8A:3...	http://mize/Data/Thalia/ACL/activex/delfile2.CAB
⊞	□	activex-delfile2.ocx-9A:52:0B:0F:CC:0D:88:FC:C2:73:94:B...	http://mize/Data/Thalia/ACL/activex/delfile2.ocx
⊞	□	activex-filebackup.CAB-81:C2:86:4F:DB:FE:5C:4A:6E:EA:8...	http://mize/Data/Thalia/ACL/activex/filebackup.CAB
⊞	□	activex-httpConnect_cpp.exe-2A:AD:9E:16:0E:83:46:2A:F...	http://mize/Data/Thalia/ACL/exe/Network/httpConnect_cpp....

Page: 1

To: Select entry...

Figure 3-34: Auto-generated Screen: Example

4. In the **Find All** field, enter the word **Java** and click **Go.**

5. Select all the found entries. In the **To** field, select the Blocked List.

6. Click **Save** and .

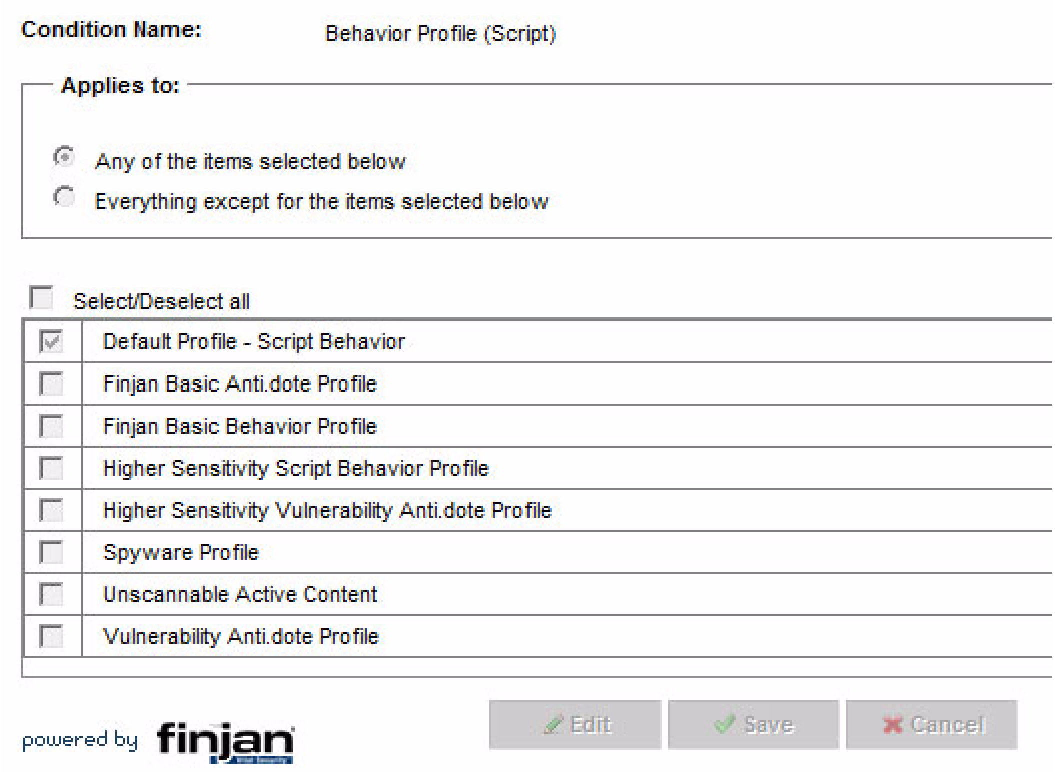
7. Re-access the Java Applets using the site, in our example:

   http://java.sun.com/applets/jdk/1.3/

This will result in an access denied message.

Block Known Spyware (CLSID)

The **Block Known Spyware (CLSID)** rule is designed to stop Spyware by detecting usage of known Spyware CLSID. CLSID is the unique identifying number of the Spyware in question.



Condition Name: Behavior Profile (Script)

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

☑	Default Profile - Script Behavior
□	Finjan Basic Anti.dote Profile
□	Finjan Basic Behavior Profile
□	Higher Sensitivity Script Behavior Profile
□	Higher Sensitivity Vulnerability Anti.dote Profile
□	Spyware Profile
□	Unscannable Active Content
□	Vulnerability Anti.dote Profile

Figure 3-35: Block Known Spyware (CLSID)

The following table displays the Rule Editor definitions:

Block Known Spyware (CLSID)	
Action	Block
End-User Message	Spyware Behavior Detected
Condition	

Block Known Spyware (CLSID)	
True Content Types	Java Script, MS Encoded Java Script, Text File, VB Script, Web Page
Behavior Profile (Script)	Spyware Profile

Rule Demonstration:

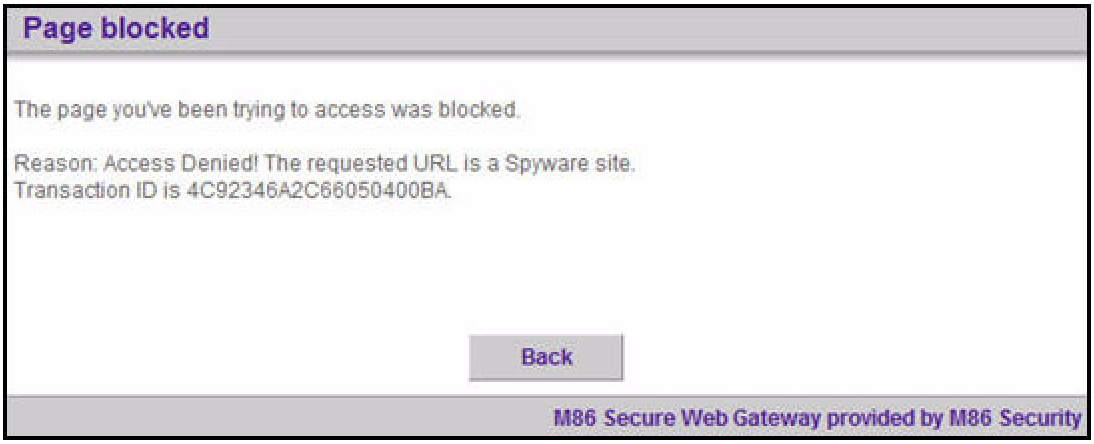
➲ **To test the Block Known Spyware (CLSID) rule:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/clsid_Spyware_demo.html

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

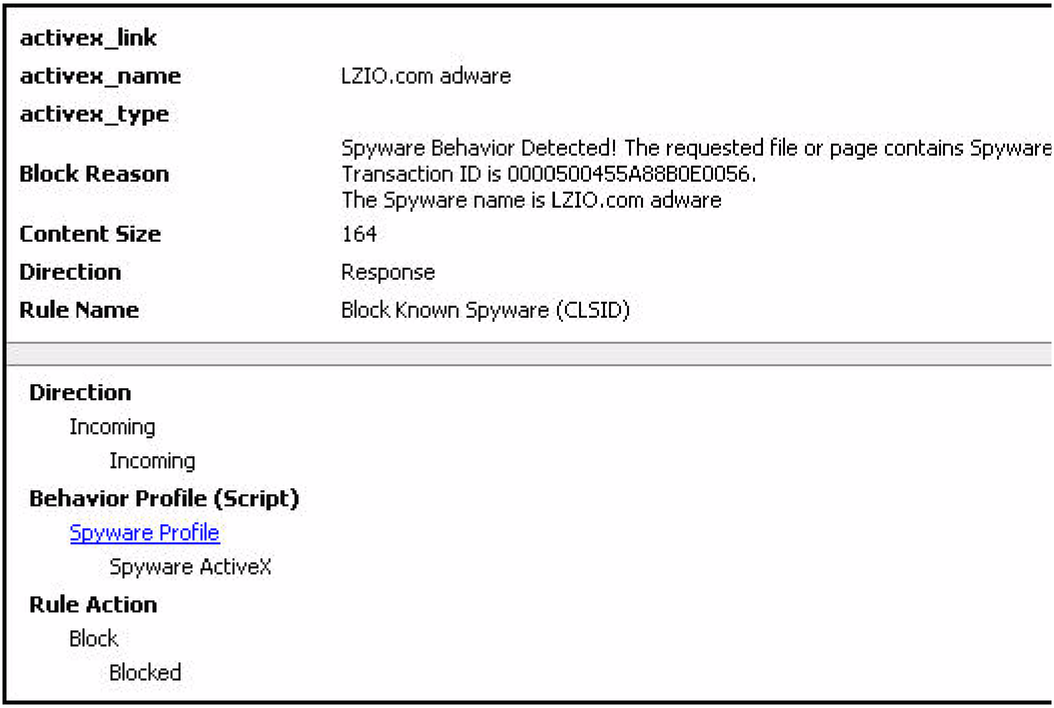
Reason: Access Denied! The requested URL is a Spyware site.
Transaction ID is 4C92346A2C66050400BA.

Figure 3-36: Page Blocked - Spyware Behavior

3. Return to the Management Console and select the **Logs** → **View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details..

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



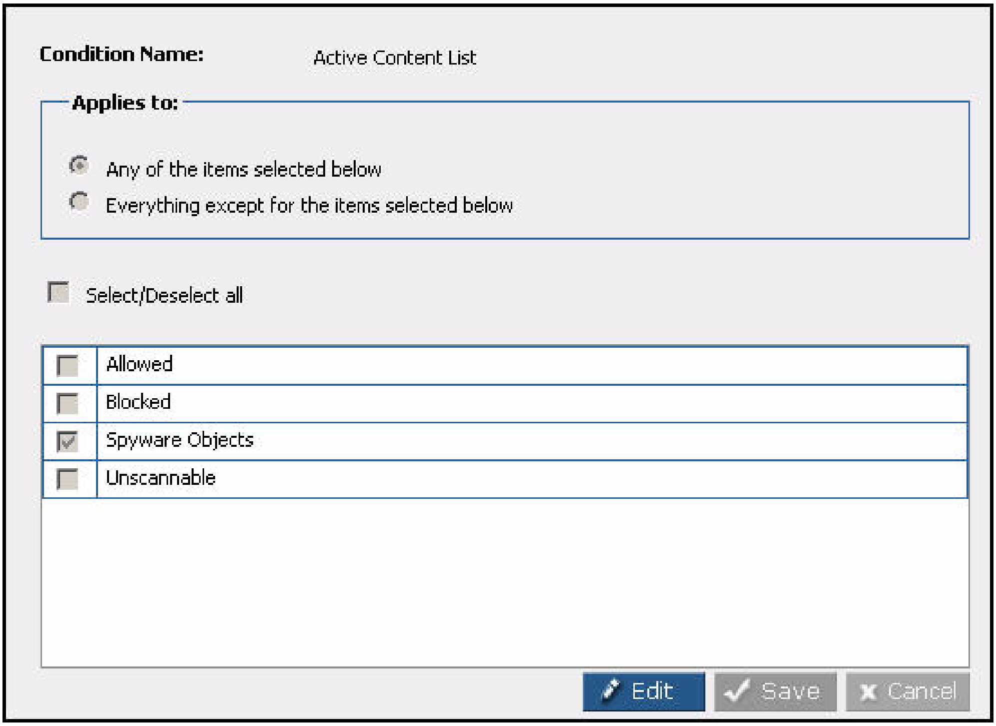
activex_link	
activex_name	LZIO.com adware
activex_type	
Block Reason	Spyware Behavior Detected! The requested file or page contains Spyware Transaction ID is 0000500455A88B0E0056. The Spyware name is LZIO.com adware
Content Size	164
Direction	Response
Rule Name	Block Known Spyware (CLSID)

Direction
Incoming
Incoming
Behavior Profile (Script)
Spyware Profile
Spyware ActiveX
Rule Action
Block
Blocked

Figure 3-37: Response: Spyware Behavior

Block Known Spyware (ACL)

The **Block Known Spyware (ACL)** refers to blocking a list of predefined malicious content. This list is generated by M86 and is not accessible by the administrator.



Condition Name: Active Content List

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

□	Allowed
□	Blocked
☑	Spyware Objects
□	Unscannable

Figure 3-38: Block Known Spywares

The following table displays the Rule Editor definitions:

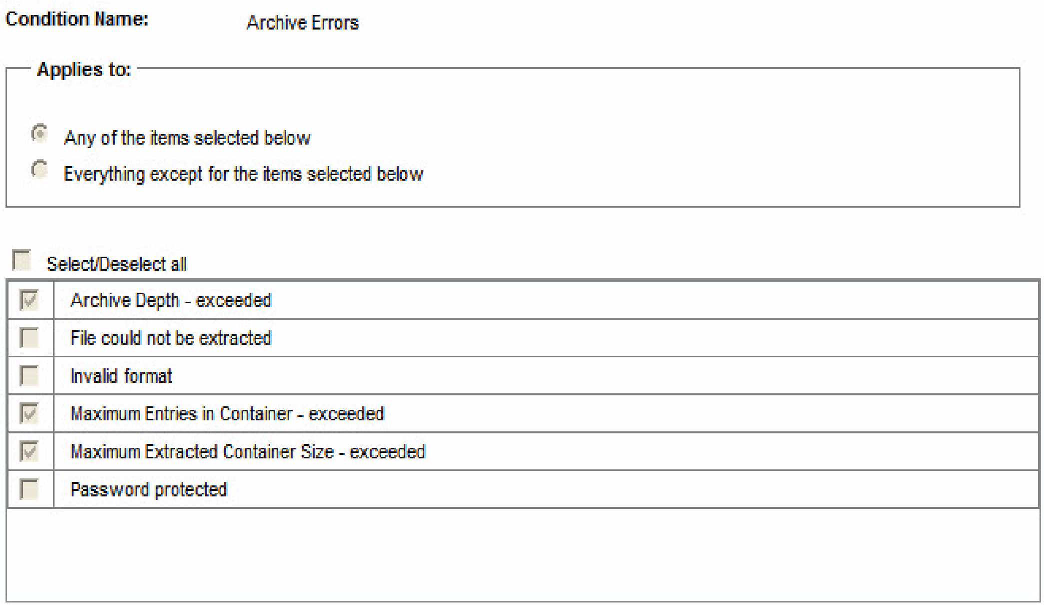
Block Known Spyware (ACL)	
Action	Block
End-User Message	Spyware Object Detected
Conditions	
True Content Type	Active binary content
Active Content List	Spyware Objects

Further Information:

- The **Block Known Spyware (ACL)** rule will be enforced, if its conditions were met, at the Response phase.

Block Potentially Malicious Archives

The **Block Potentially Malicious Archives** rule was designed to block attacks that try to cause Denial of Service using archives.



Condition Name: Archive Errors

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

☑	Archive Depth - exceeded
□	File could not be extracted
□	Invalid format
☑	Maximum Entries in Container - exceeded
☑	Maximum Extracted Container Size - exceeded
□	Password protected

Figure 3-39: Block Potentially Malicious Archives

The following table displays the Rule Editor definitions:

Block Potentially Malicious Archives	
Action	Block
End-User Message	Container Violation
Conditions	
Archive Errors	Maximum Extracted Container Size - exceeded, Archive Depth - exceeded, Maximum Entries in Container - exceeded

Rule Demonstration

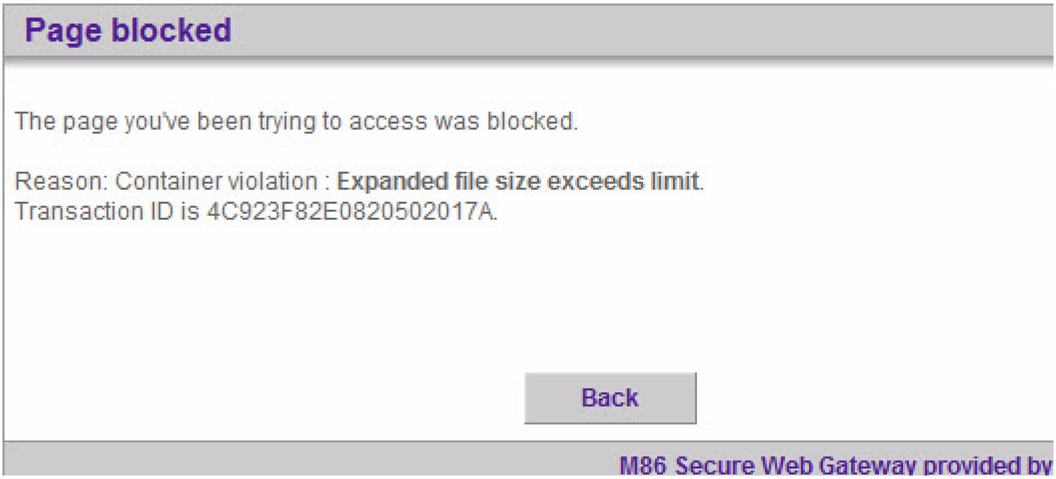
➲ **To test the Block Potentially Malicious Archives rule:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/Potentially_Malicious_Archives_Demo.zip

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

After the downloading box, the following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

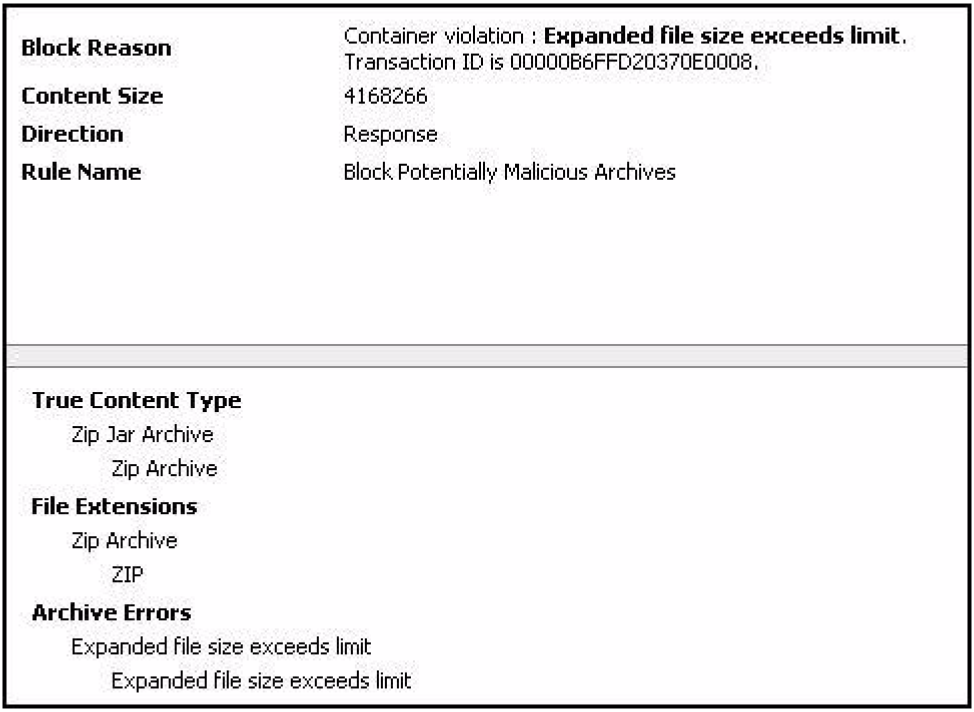
Reason: Container violation : **Expanded file size exceeds limit**.
Transaction ID is 4C923F82E0820502017A.

Figure 3-40: Page Blocked: Potentially Malicious Archives

3. Return to the Management Console and select the **Logs** → **View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▸☰ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	Container violation : **Expanded file size exceeds limit**. Transaction ID is 00000B6FFD20370E0008.
Content Size	4168266
Direction	Response
Rule Name	Block Potentially Malicious Archives

True Content Type

- Zip Jar Archive
  - Zip Archive

File Extensions

- Zip Archive
  - ZIP

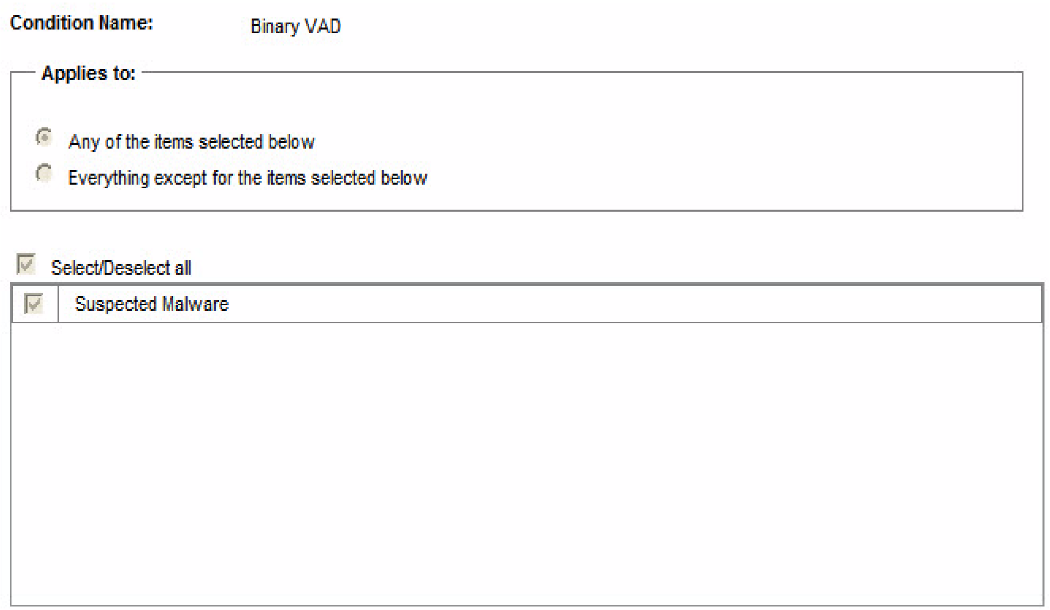
Archive Errors

- Expanded file size exceeds limit
  - Expanded file size exceeds limit

Figure 3-41: Response: Block Potentially Malicious Archives

Block Binary VAD Vulnerabilities

The **Block Binary VAD Vulnerabilities** rule blocks binary application level vulnerabilities based on MCRC detection rules.



Condition Name: Binary VAD

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

☑ Select/Deselect all

☑ Suspected Malware

Figure 3-42: Block Binary VAD Vulnerabilities

The following table displays the definitions:

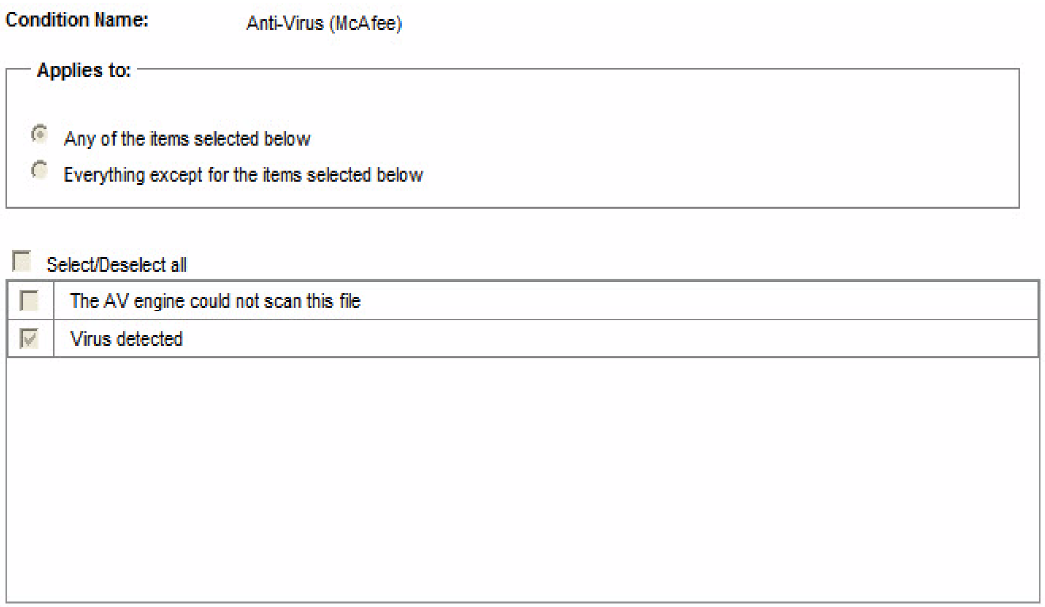
Block Binary VAD Vulnerabilities	
Action	Block
End-User Message	Binary VAD Violation
Conditions	
Binary VAD	Suspected Malware

Further Information:

- The **Suspected Malware** list is constantly updated by MCRC and cannot be accessed by the administrator.

Block Known Viruses (McAfee / Sophos / Kaspersky)

The **Block Known Viruses (McAfee/Sophos/Kaspersky)** rule blocks known viruses using the Anti-Virus engine that you have a license for and provides a specific virus name in the Web Logs where possible. There are three Anti-Virus engines – McAfee, Sophos and Kaspersky – that work with the SWG Appliance. Using an Anti-Virus engine helps to optimize user experience.



Condition Name: Anti-Virus (McAfee)

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□	The AV engine could not scan this file
☑	Virus detected

Figure 3-43: Block Known Viruses (McAfee/Sophos/Kaspersky) rule

The following table displays the Rule definitions:

Block Known Viruses	
Action	Block
End-User Message	Virus detected

Block Known Viruses	
Conditions	
Anti-Virus (McAfee/ Sophos/Kaspersky)	Virus detected

Rule Demonstration:

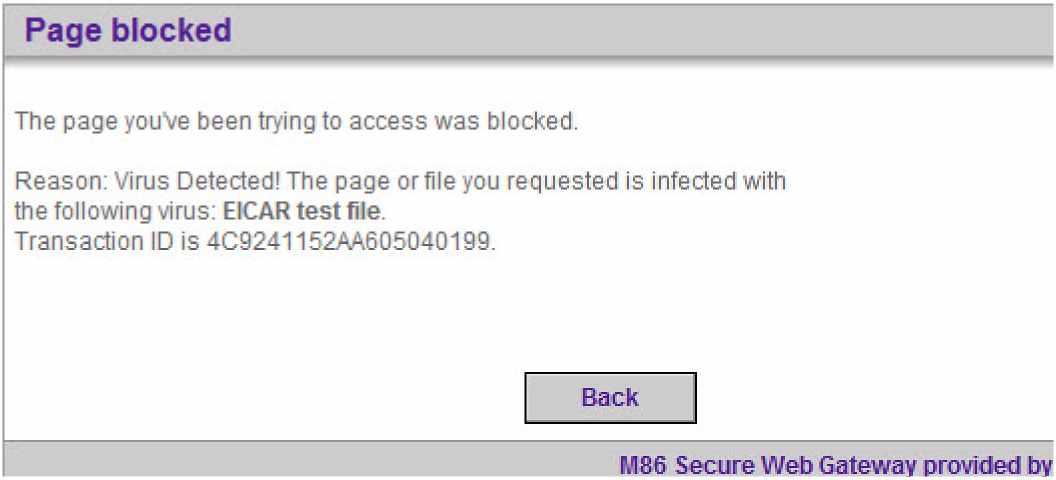
➲ **To test the Block Known Viruses (McAfee/Sophos/Kaspersky) rule:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/eicar.com.txt

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

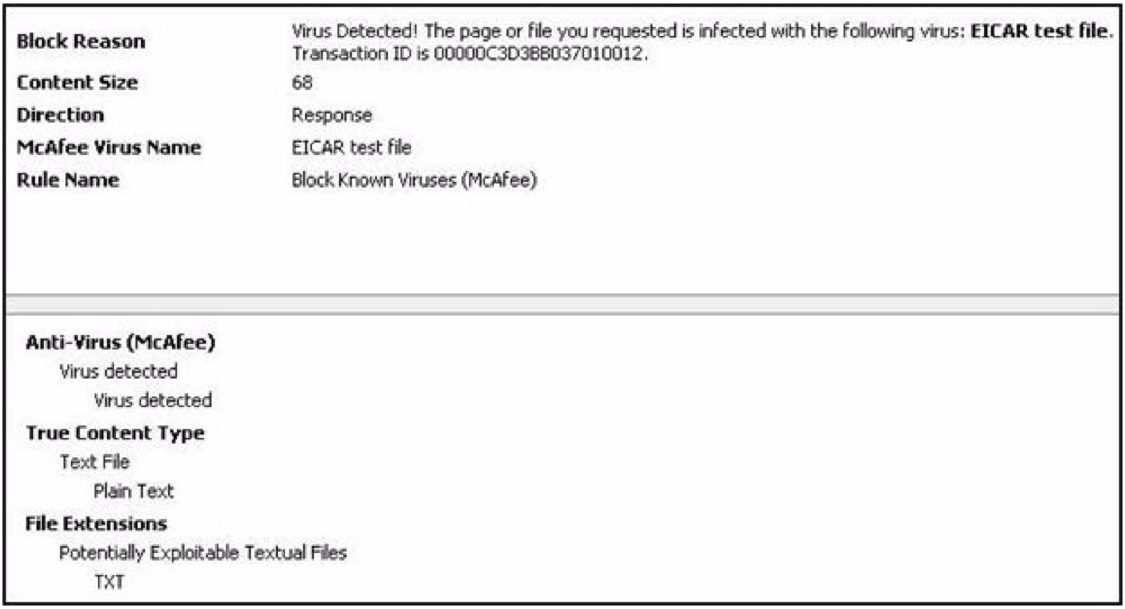
Reason: Virus Detected! The page or file you requested is infected with the following virus: EICAR test file.
Transaction ID is 4C9241152AA605040199.

Figure 3-44: Page Blocked: Virus

3. Return to the Management Console and select the **Logs** → **View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	Virus Detected! The page or file you requested is infected with the following virus: **EICAR test file**. Transaction ID is 00000C3D3BB037010012.
Content Size	68
Direction	Response
McAfee Virus Name	EICAR test file
Rule Name	Block Known Viruses (McAfee)

Anti-Virus (McAfee)
- Virus detected
  - Virus detected

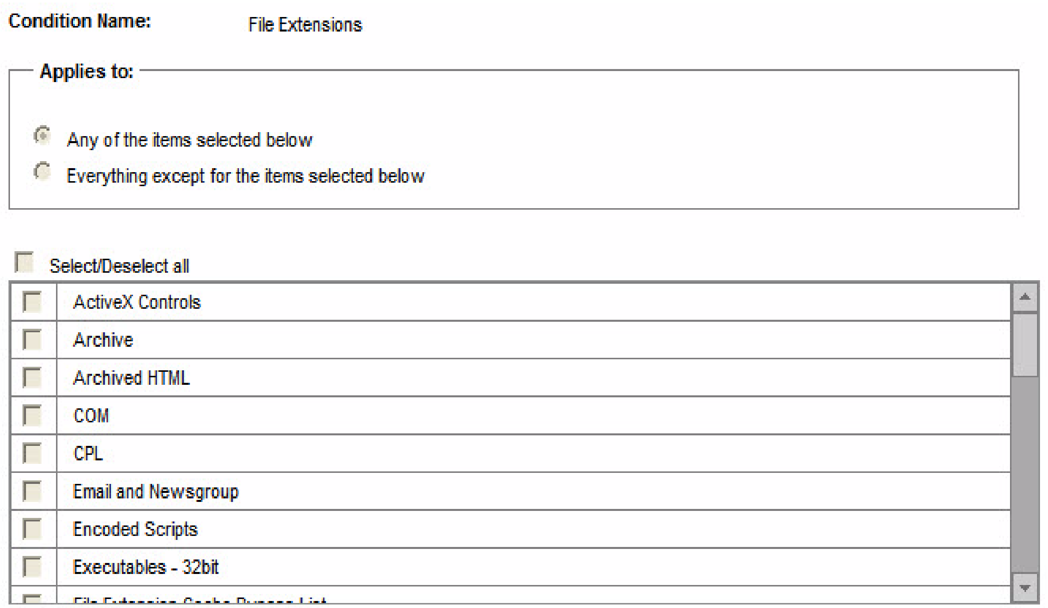
True Content Type
- Text File
  - Plain Text

File Extensions
- Potentially Exploitable Textual Files
  - TXT

Figure 3-45: Response - Virus Detected

Block Customer-Defined File Extensions

The **Block Customer-Defined File Extensions** rule only appears in the M86 Basic Security Policy and is only relevant if you selected file extensions through the Simplified Policies interface.



Condition Name: File Extensions

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□ ActiveX Controls

□ Archive

□ Archived HTML

□ COM

□ CPL

□ Email and Newsgroup

□ Encoded Scripts

□ Executables - 32bit

□ File Extension Cache Bypass List

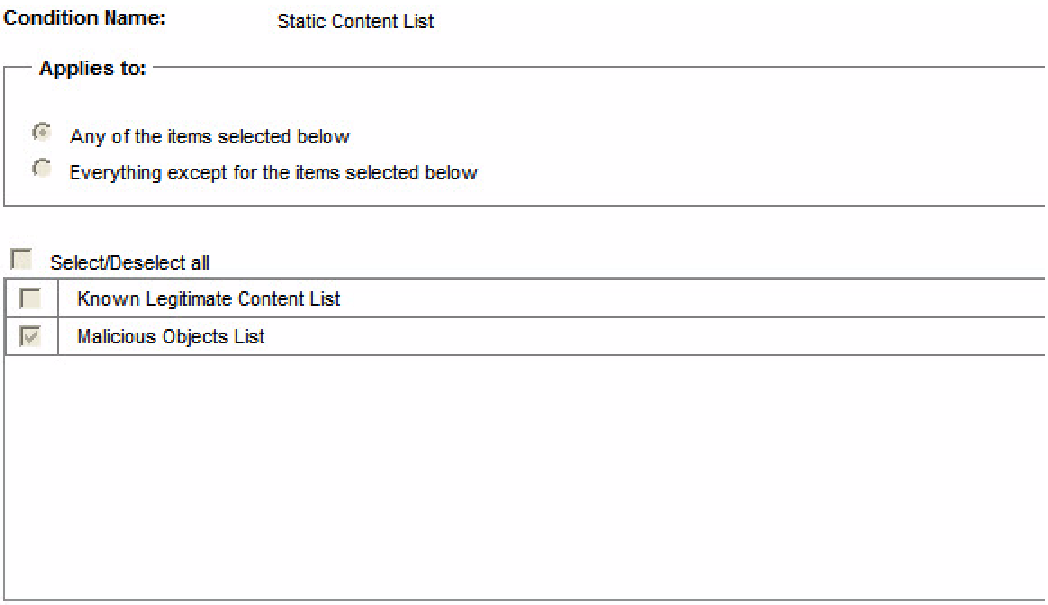
Figure 3-46: Block Customer-Defined File Extensions

The following table displays the Rule definitions:

Block Customer-Defined File Extensions	
Action	Block
End-User Message	File Extension
Conditions	
File Extensions	Block File Extensions (Basic)

Block Known Malicious Content

The **Block Known Malicious Content** rule refers to blocking a list of predefined Malicious Objects by statically blocking malicious objects which were identified as such by M86's MCRC team.



Condition Name: Static Content List

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

□	Known Legitimate Content List
☑	Malicious Objects List

Figure 3-47: Block Known Malicious Content

The following table displays the definitions:

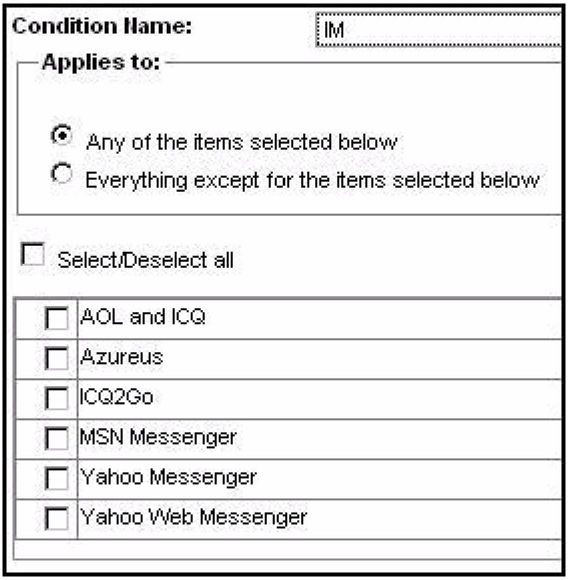
Block Known Malicious Content	
Action	Block
End-User Message	Hash Scanner
Conditions	
Static Content List	Malicious Objects List

Further Information:

- The Malicious Objects List cannot be manipulated or viewed by the administrator.

Block IM Tunneling

The **Block IM Tunneling** rule blocks IM tunneling by default since these are known crimeware distribution vehicles.



Condition Name: IM

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

□ AOL and ICQ
□ Azureus
□ ICQ2Go
□ MSN Messenger
□ Yahoo Messenger
□ Yahoo Web Messenger

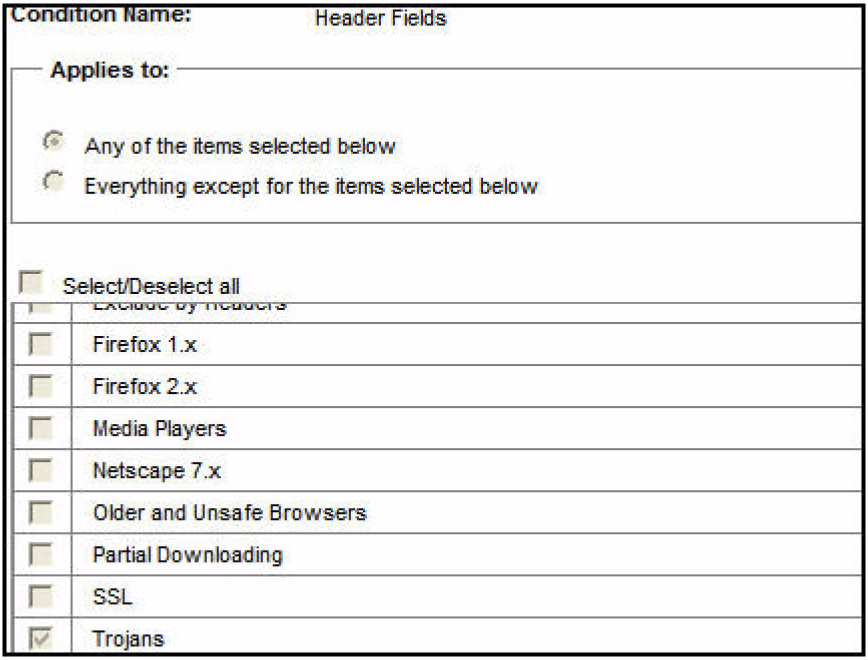
Figure 3-48: Block IM Tunneling rule

The following table displays the definitions:

Block IM Tunneling	
Action	Block
Reason	Instant Messenger Detected
Conditions	
IM	AOL and ICQ/ MSN Messenger/Yahoo Messenger

Detect Known Trojan Network Activity

The **Detect Known Trojan Network Activity** rule detects network activity usually associated with Trojans sending and receiving data from the Internet. This rule is provided in X-Ray format with the predefined Security Policies. To change this rule to block Trojan activity, duplicate the Policy and remove the check in the X-Ray checkbox.



Condition Name: Header Fields

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□ Exclude by Headers

□ Firefox 1.x

□ Firefox 2.x

□ Media Players

□ Netscape 7.x

□ Older and Unsafe Browsers

□ Partial Downloading

□ SSL

☑ Trojans

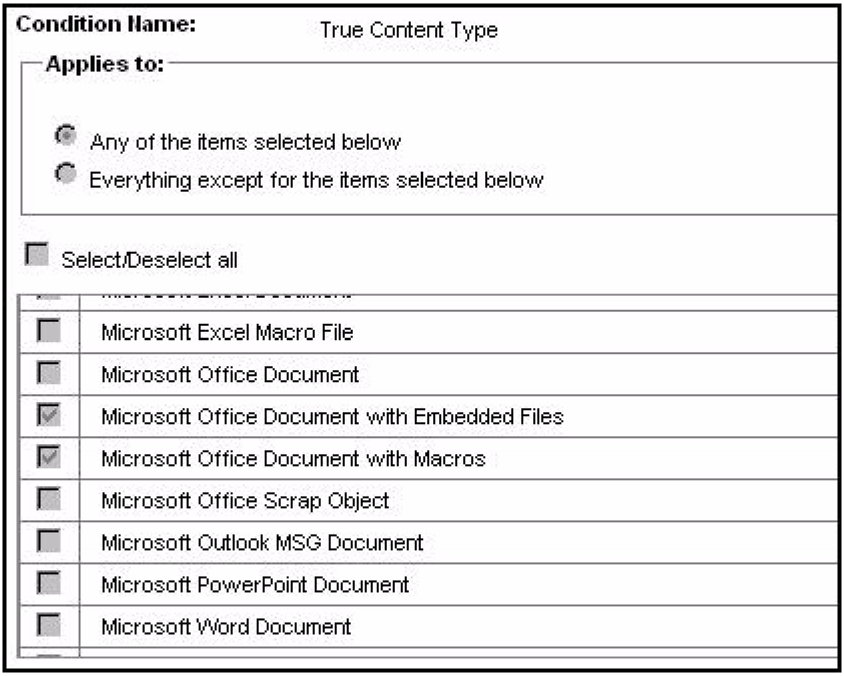
Figure 3-49: Detect Known Trojan Network Activity

The following table displays the definitions:

Detect Known Trojan Network Activity	
Action	Block
End-User Message	Suspected Trojan traffic detected (appears in Logs on X-Ray action)
Condition	
Header Fields	Trojans
Direction	Outgoing

Block Microsoft Office Documents containing Macros and/or Embedded Files

The **Block Microsoft Office Documents containing Macros and/or Embedded files** rule blocks Microsoft Office Documents which contain macros or embedded files. This is because macros and embedded files might contain malicious code.



Condition Name: True Content Type

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□	Microsoft Excel Macro File
□	Microsoft Office Document
☑	Microsoft Office Document with Embedded Files
☑	Microsoft Office Document with Macros
□	Microsoft Office Scrap Object
□	Microsoft Outlook MSG Document
□	Microsoft PowerPoint Document
□	Microsoft Word Document

Figure 3-50: Block Microsoft Office Documents containing Macros and/or Embedded files rule

The following table displays the definitions:

Block Microsoft Office Documents containing Macros and/or Embedded file	
Action	Block
End-User Message	Suspicious File Type Detected
Conditions	
True Content Type	Microsoft Office Document with Embedded Files, Microsoft Office Document with Macros

Rule Demonstration

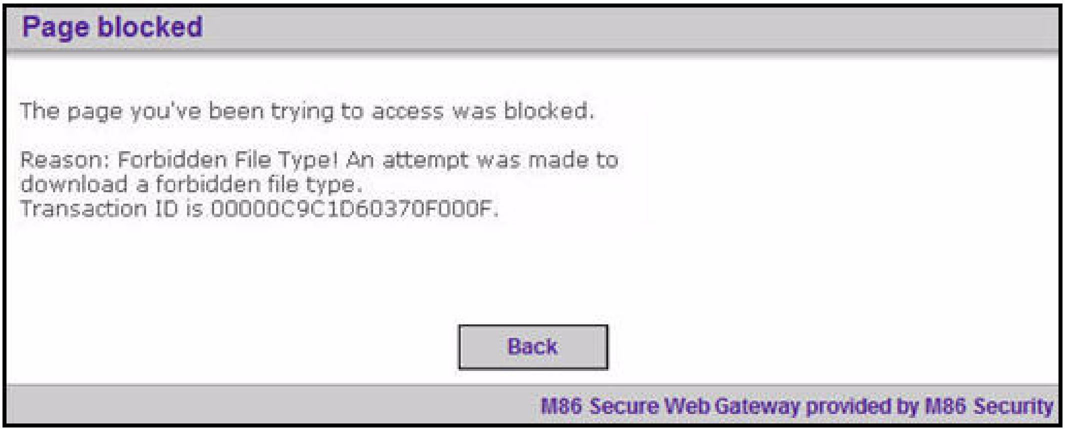
➲ **To test the Block Microsoft Office Documents containing Macros and/or Embedded files rule:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/macro.doc

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following message appears:



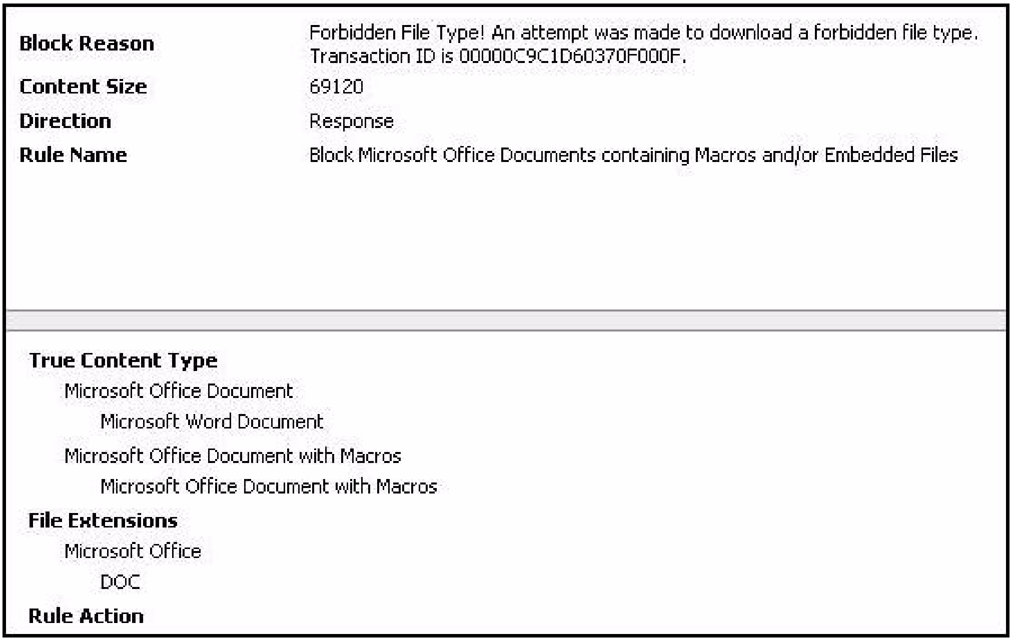
Page blocked

The page you've been trying to access was blocked.

Reason: Forbidden File Type! An attempt was made to download a forbidden file type.
Transaction ID is 00000C9C1D60370F000F.

Figure 3-51: Page Blocked - Microsoft Office document containing macro

3. Return to the Management Console and select the **Logs** → **View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click ☰ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	Forbidden File Type! An attempt was made to download a forbidden file type. Transaction ID is 00000C9C1D60370F000F.
Content Size	69120
Direction	Response
Rule Name	Block Microsoft Office Documents containing Macros and/or Embedded Files

True Content Type

- Microsoft Office Document
  - Microsoft Word Document
- Microsoft Office Document with Macros
  - Microsoft Office Document with Macros

File Extensions

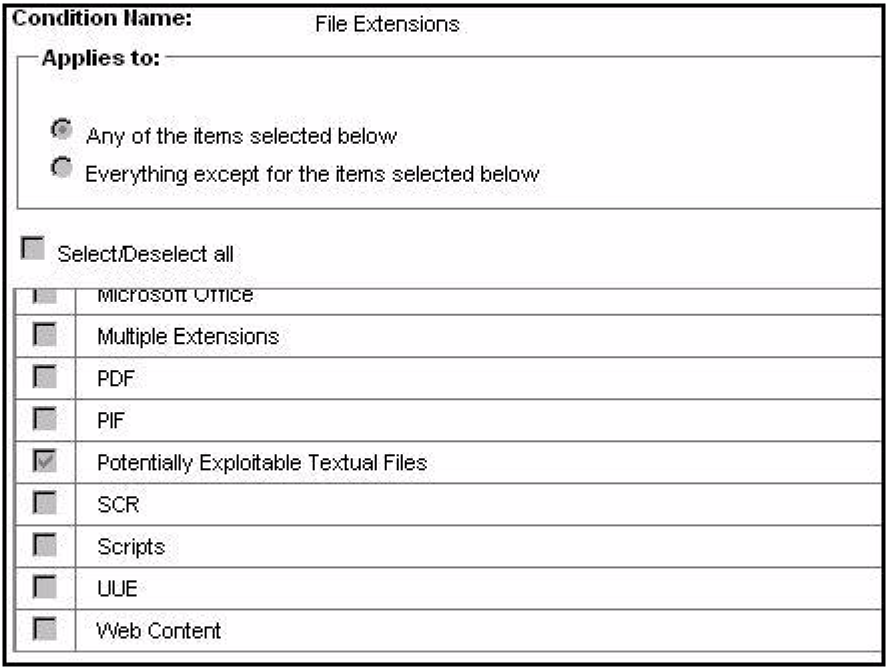
- Microsoft Office
  - DOC

Rule Action

Figure 3-52: Response: Microsoft Office document with Macros

Block Binary Exploits in Textual Files

The **Block Binary Exploits in Textual Files** rule blocks potential exploitations of vulnerable applications by detecting and blocking textual files with binary data.



Condition Name: File Extensions

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□	Microsoft Office
□	Multiple Extensions
□	PDF
□	PIF
☑	Potentially Exploitable Textual Files
□	SCR
□	Scripts
□	UUE
□	Web Content

Figure 3-53: Block Binary Exploits in Textual Files

The following table displays the Rule definitions:

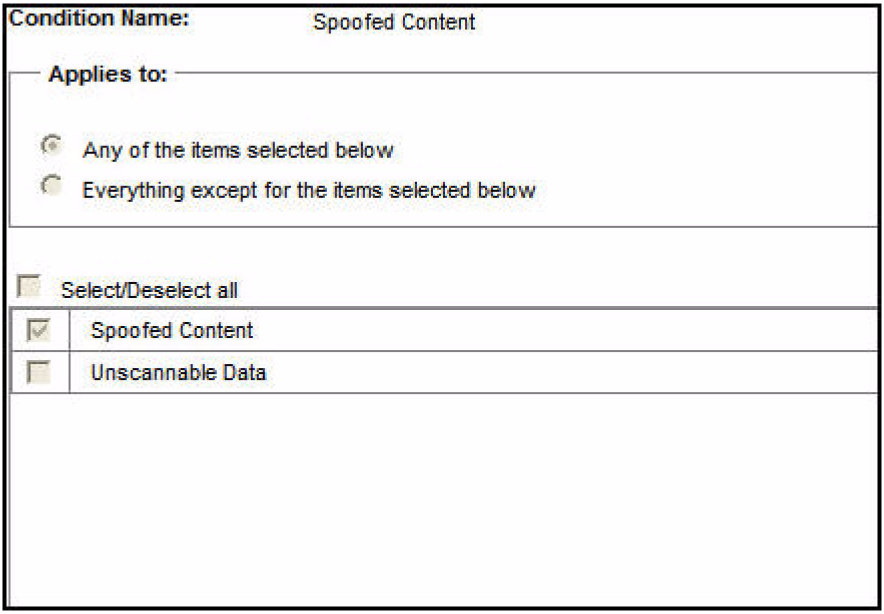
Block Binary Exploits in Textual Files	
Action	Block
End-User Message	Blocked Binary Exploit in Textual File
Conditions	
Content Size	Greater than 0 MB
File Extensions	Potentially Exploitable Textual Files
True Content Type	Unscannable Data

Further information:

- True Content Type: Unscannable data refers to binary content in a textual file.
- The Potentially Exploitable Textual Files list can be viewed under **Policies → Condition Settings → File extensions**.

Block Spoofed Content

The **Block Spoofed Content** rule was designed to neutralize attacks in which a virus or malicious code masquerades as a harmless file in order to elude the anti-virus engine. This rule also covers situations where executable files are spoofed as other extension files.



Condition Name: Spoofed Content

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

☑ Spoofed Content

□ Unscannable Data

Figure 3-54: Spoofed Content Filtering rule

The following table displays the definitions:

Block Spoofed Content	
Action	Block
End-User Message	Spoofed Content Detected
Conditions	
Spoofed Content	Spoofed Content

Rule Demonstration:

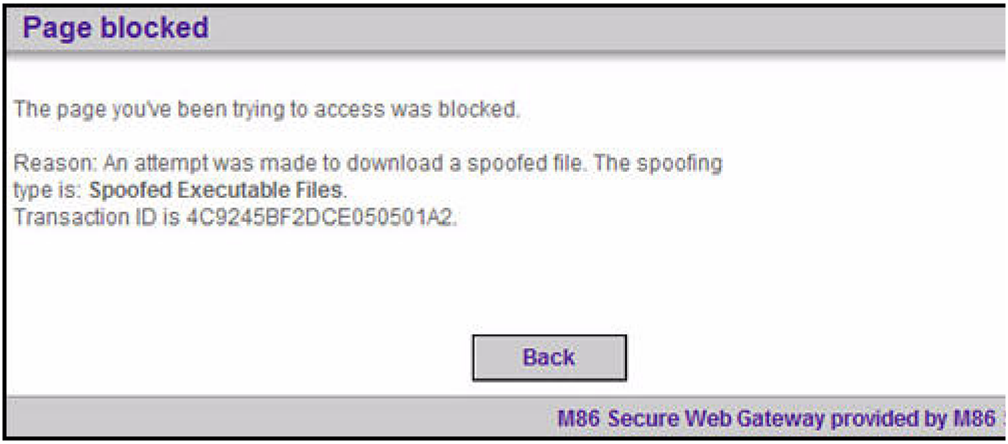
➲ **To test the Block Spoofed Content rule:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/archive.zip

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following message appears:



Page blocked

The page you've been trying to access was blocked.

Reason: An attempt was made to download a spoofed file. The spoofing type is: Spoofed Executable Files.
Transaction ID is 4C9245BF2DCE050501A2.

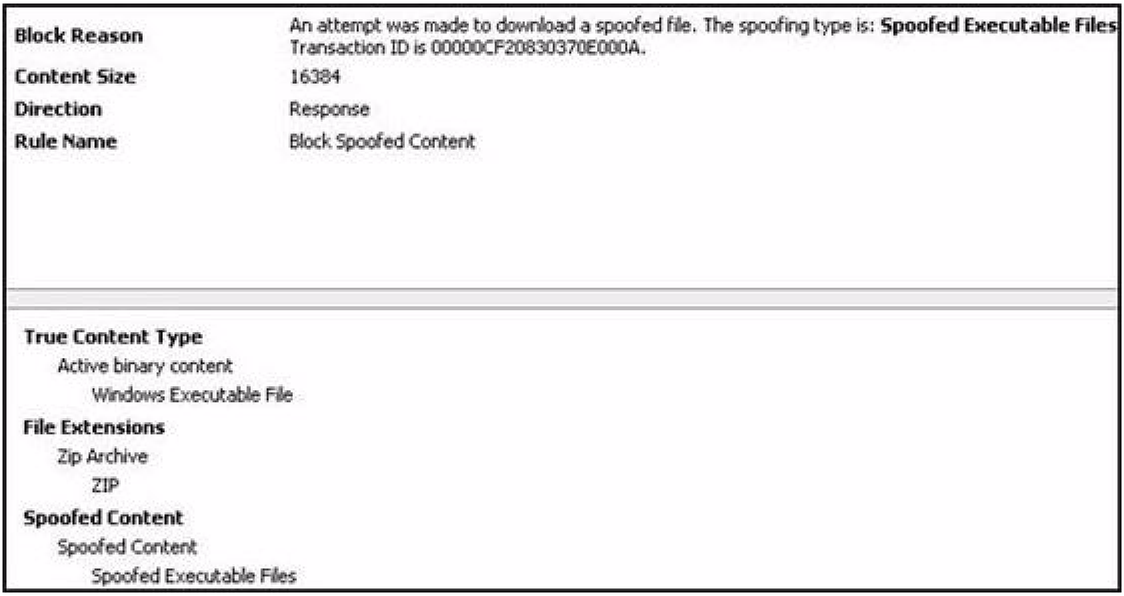
M86 Secure Web Gateway provided by M86

Figure 3-55: Page Blocked: Spoofed Content

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason An attempt was made to download a spoofed file. The spoofing type is: **Spoofed Executable Files** Transaction ID is 00000CF20830370E000A.

Content Size 16384

Direction Response

Rule Name Block Spoofed Content

True Content Type
Active binary content
Windows Executable File

File Extensions
Zip Archive
ZIP

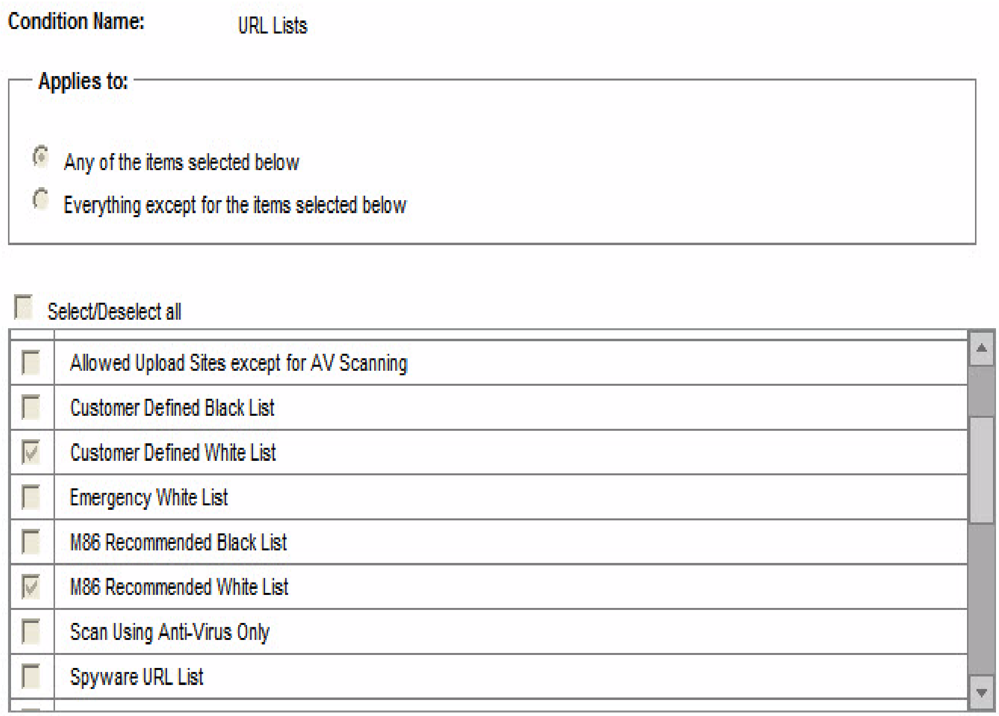
Spoofed Content
Spoofed Content
Spoofed Executable Files

Figure 3-56: Response: Block Spoofed Content

Allow Access to White Listed Sites

The **Allow Access to White Listed Sites** rule allows through sites added to safe lists - but files within containers that may reside on the sites are still scanned.

White lists can be used to prevent over-blocking caused by detection of dangerous operation in an active content which is required for the productivity of the organization, e.g. Microsoft Windows update sites which contain a powerful ActiveX control. White lists can therefore be used as performance accelerators when browsing trusted sites.



Condition Name: URL Lists

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

- □ Allowed Upload Sites except for AV Scanning
- □ Customer Defined Black List
- ☑ Customer Defined White List
- □ Emergency White List
- □ M86 Recommended Black List
- ☑ M86 Recommended White List
- □ Scan Using Anti-Virus Only
- □ Spyware URL List

Figure 3-57: Allow Access to White Listed Sites

The following table displays the definitions:

Allow Access to White Listed Sites	
Action	Allow content and scan containers
Conditions	
URL Lists	URL White List (Basic/Medium/Strict), M86 Recommended White List, Customer Defined White List

Further information:

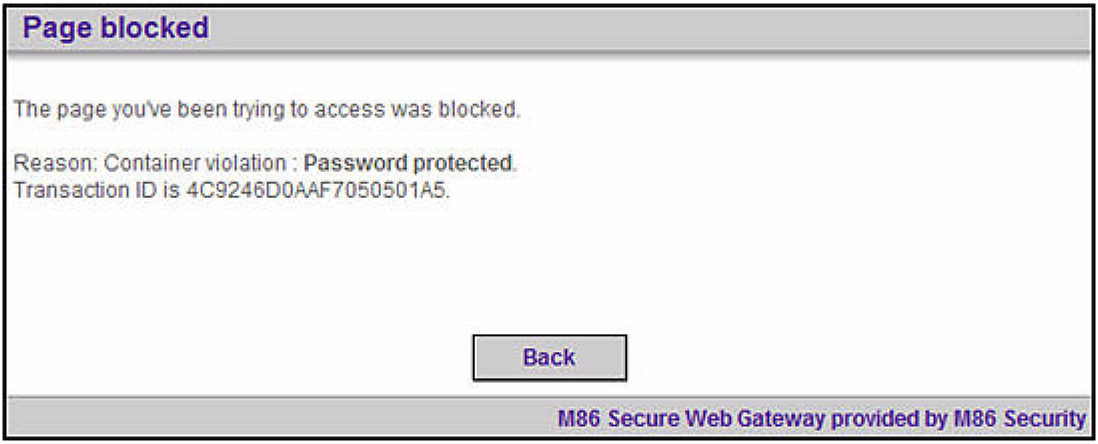
- The M86 Recommended White List cannot be edited by the user.
- The Customer Defined White List is available at **Policies → Condition Settings →URL Lists**. This can be edited by the administrator.
- The URL White List can be edited via the Simplified Interface.

Rule Demonstration:

➲ To test the Allow Access to White Listed Sites rule:

1. First, let's find a URL site that is blocked. Copy and paste the following URL into your browser. http://www.m86security.com/EVG/passwordprotected.zip
2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The URL is blocked since it contains a password protected archive. The following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

Reason: Container violation : **Password protected**.
Transaction ID is 4C9246D0AAF7050501A5.

M86 Secure Web Gateway provided by M86 Security

Figure 3-58: Page Blocked – Password Protected

In order to avoid blocking this page we can add it to the White List.

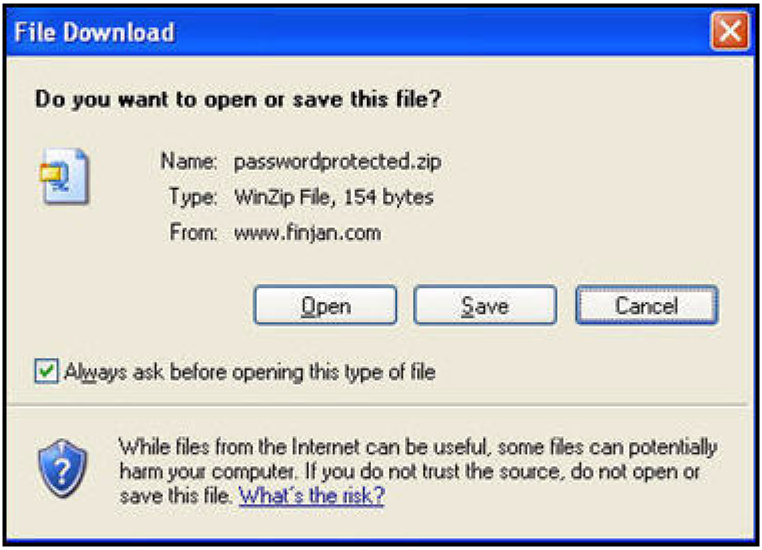
➲ **To add this page to the White List:**

1. Open the Customer Defined White List by navigating to **Policies →Condition Settings →URL Lists→ Customer Defined White List.**
2. Click **Edit** at the bottom right of the screen.
3. Click ✚ to add a row. Enter the following :

   `www.finjan.com/EVG/passwordprotected.zip.`

4. Click **Save** and click ✔ .
5. Once again, copy and paste the following URL into your browser: http://www.m86security.com/EVG/passwordprotected.zip

To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**. The following screen is displayed:



File Download

Do you want to open or save this file?

Name: passwordprotected.zip
Type: WinZip File, 154 bytes
From: www.finjan.com

☑ Always ask before opening this type of file

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 3-59: Web Site from White List

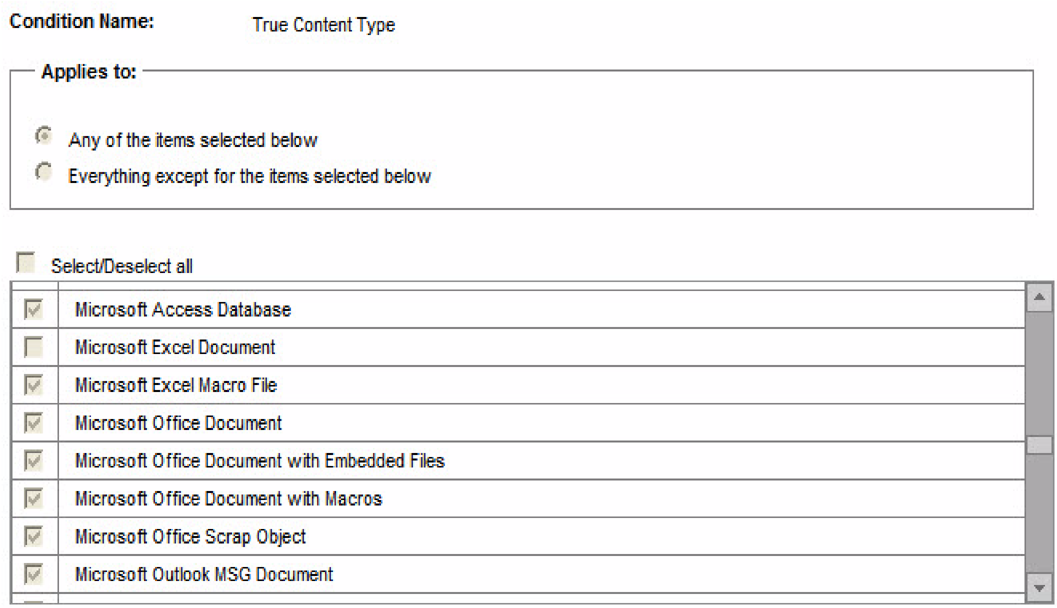
6. Click **Open** and the file is downloaded.

➲ **To delete the page from the White List:**

1. Navigate to **Policies → Condition Settings → URL Lists→ Customer Defined White List**.
2. Click next to the www.m86security.com/EVG/ passwordprotected.zip entry, and select **Delete**.
3. After deleting the entry, click both **Save** and .

Block Outgoing Microsoft Office Documents

The **Block Outgoing Microsoft Office Documents** logs the amount of transmission of Microsoft Office documents to the Internet. In the M86 Policy it is defined as X-Ray.



Condition Name: True Content Type

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

☐ Select/Deselect all

☑	Microsoft Access Database
☐	Microsoft Excel Document
☑	Microsoft Excel Macro File
☑	Microsoft Office Document
☑	Microsoft Office Document with Embedded Files
☑	Microsoft Office Document with Macros
☑	Microsoft Office Scrap Object
☑	Microsoft Outlook MSG Document

Figure 3-60: Block Outgoing Microsoft Office Document

The following table displays the Rule definitions:

Block Outgoing Microsoft Office Documents	
Action	Block (X-Ray)
End-User Message	Outgoing Microsoft Office File Detection (N/A)
Conditions	
Direction	Outgoing
File Extensions	Microsoft Office
True Content Type	Microsoft Office Document, Microsoft Office Document with Embedded Files, Microsoft Office Document with Macros, Microsoft Office Scrap Object, Microsoft Outlook MSG Document, Microsoft Word document, Microsoft Excel Macro File, Microsoft Access Database

Further Information:

- The **Block Outgoing Microsoft Office Documents** rule has been added as an X-ray rule in the predefined M86 Security Policies.This means that no documents will actually be blocked; but the results will be displayed in the Logs view.
- If the **Block Outgoing Microsoft Office Documents** rule was Active, then it would be enforced, if its conditions were met, at the request phase.

Rule Demonstration:

➲ **To test the Block Outgoing Microsoft Office Documents rule:**

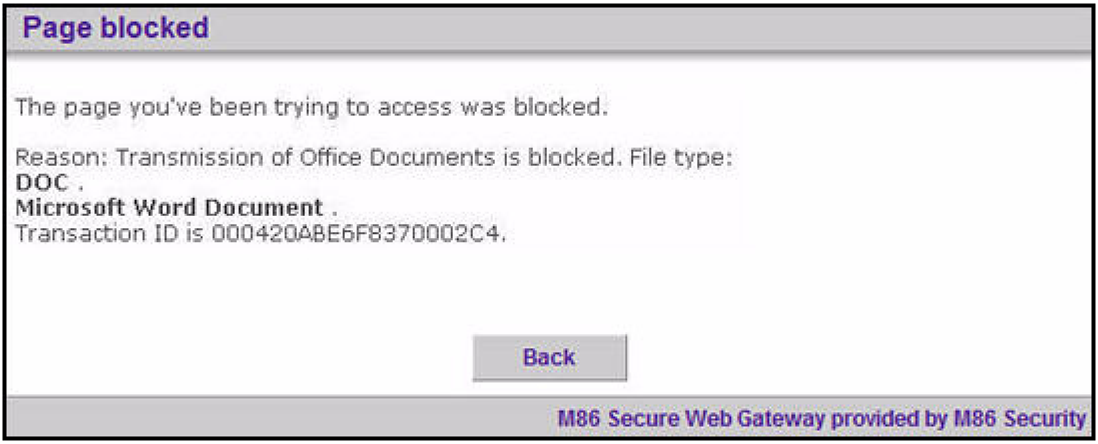
1. Duplicate the **M86 Medium Security Policy**.
2. Edit the **Block Outgoing Microsoft Office Document** rule by disabling the X-Ray checkbox.

3. Make sure your User Group has the Duplicate Policy assigned to it.

4. Copy and paste the following URL into your browser: http://encodable.com/uploaddemo/

5. In the File 1 of 1 field, select **Browse** and select any Microsoft Office document for uploading.

6. Click **Begin Uploading**. The following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

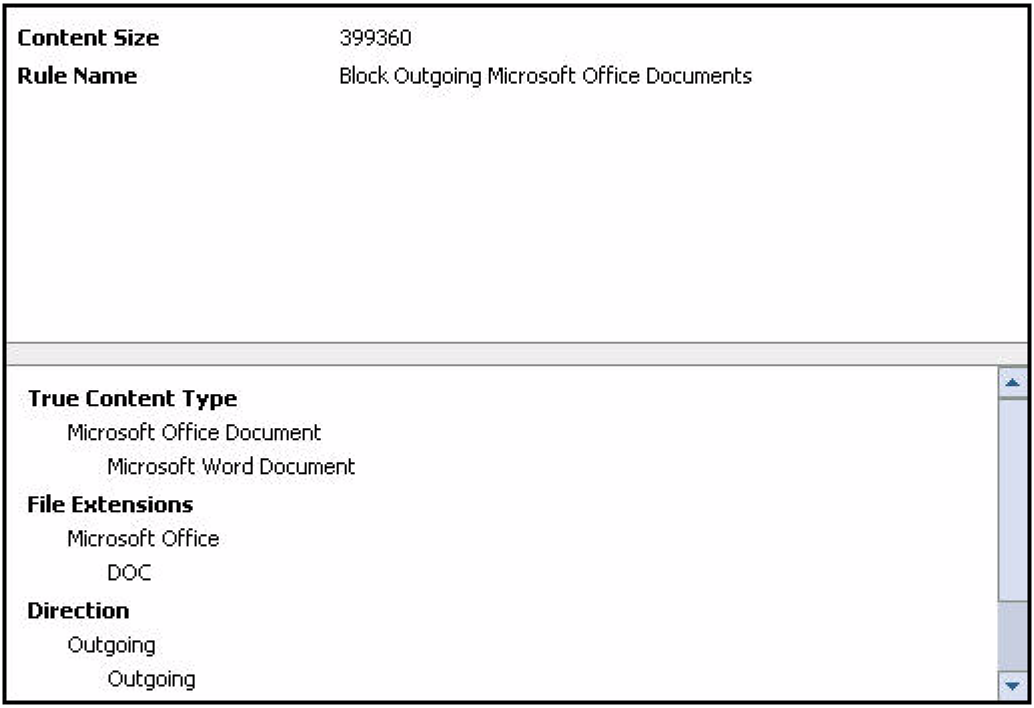
Reason: Transmission of Office Documents is blocked. File type:
DOC .
Microsoft Word Document .
Transaction ID is 000420ABE6F8370002C4.

Figure 3-61: Page Blocked - Block Outgoing Microsoft Office Documents

7. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

8. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

9. In the Transaction Details tree, click on Request (4) screen to obtain further information on the Request phase of this transaction. Only the Request component exists for this transaction since it was blocked at the request phase.



Content Size	399360
Rule Name	Block Outgoing Microsoft Office Documents

True Content Type
- Microsoft Office Document
  - Microsoft Word Document

File Extensions
- Microsoft Office
  - DOC

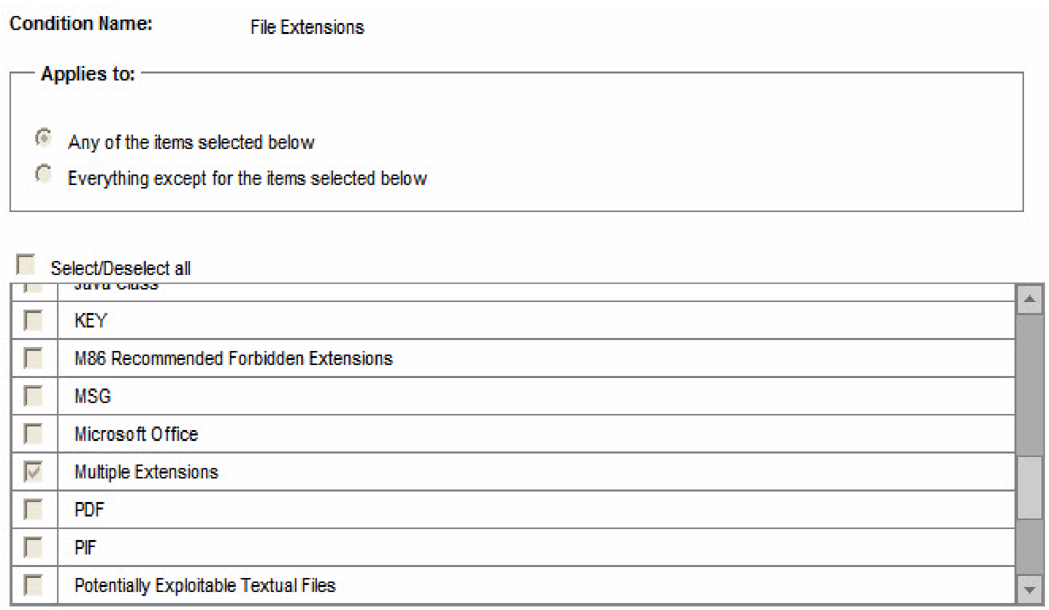
Direction
- Outgoing
  - Outgoing

Figure 3-62: Request: Block Outgoing Microsoft Office Documents

10.Reassign the required Security Policy to your User Group.

Block Files with Suspicious Multiple Extensions

The **Block Files with Suspicious Multiple Extensions** rule blocks files with suspicious multiple extensions. This is based on a comparison of the last extension to a list of suspicious extensions (as well as comparing the extension before last to a list of benign extensions). This rule was designed so that users would not download a potentially dangerous file by mistake.



Condition Name: File Extensions

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□ Java Class

□ KEY

□ M86 Recommended Forbidden Extensions

□ MSG

□ Microsoft Office

☑ Multiple Extensions

□ PDF

□ PIF

□ Potentially Exploitable Textual Files

Figure 3-63: Block Files with Suspicious Multiple Extensions

The following table displays the Rule definitions:

Block Files with Suspicious Multiple Extensions	
Action	Block
End-User Message	Multiple Extensions
Conditions	
File Extension	Multiple Extensions

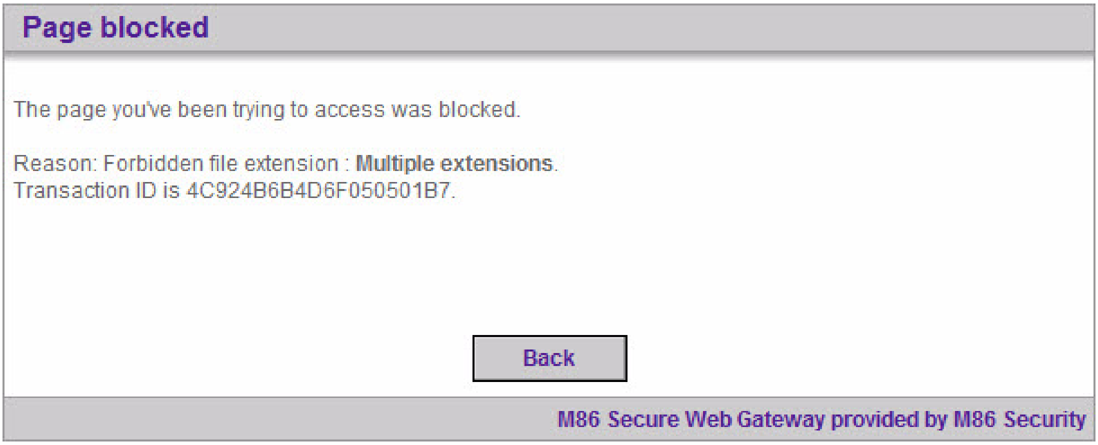
Rule Demonstration:

➲ To test the Block Files with Suspicious Multiple Extensions rule:

1. Copy and paste the following URL into your browser: http://www.m86security.com/EVG/Capitalsettime.TXT.JS

To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

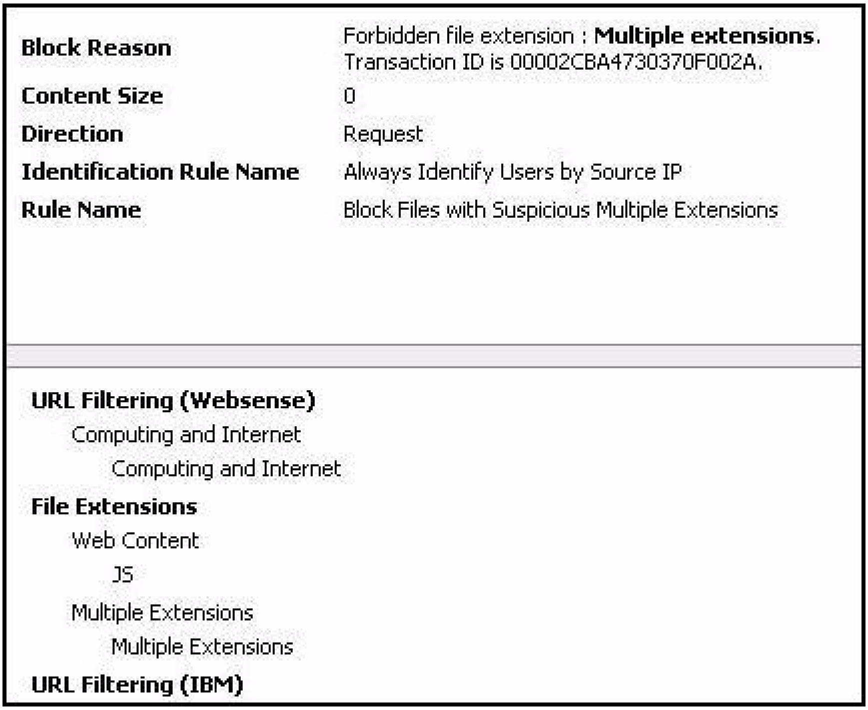
Reason: Forbidden file extension : **Multiple extensions**.
Transaction ID is 4C924B6B4D6F050501B7.

Figure 3-64: Page Blocked - Multiple Extensions

2. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

3. In the same row as the blocked transaction, click ▸ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

4. In the Transaction Details tree, click **Request** to obtain further information on the Request phase of this transaction. Only the Request component exists for this transaction since it was blocked at the request phase.



Block Reason	Forbidden file extension : **Multiple extensions**. Transaction ID is 00002CBA4730370F002A.
Content Size	0
Direction	Request
Identification Rule Name	Always Identify Users by Source IP
Rule Name	Block Files with Suspicious Multiple Extensions

URL Filtering (Websense)
- Computing and Internet
  - Computing and Internet

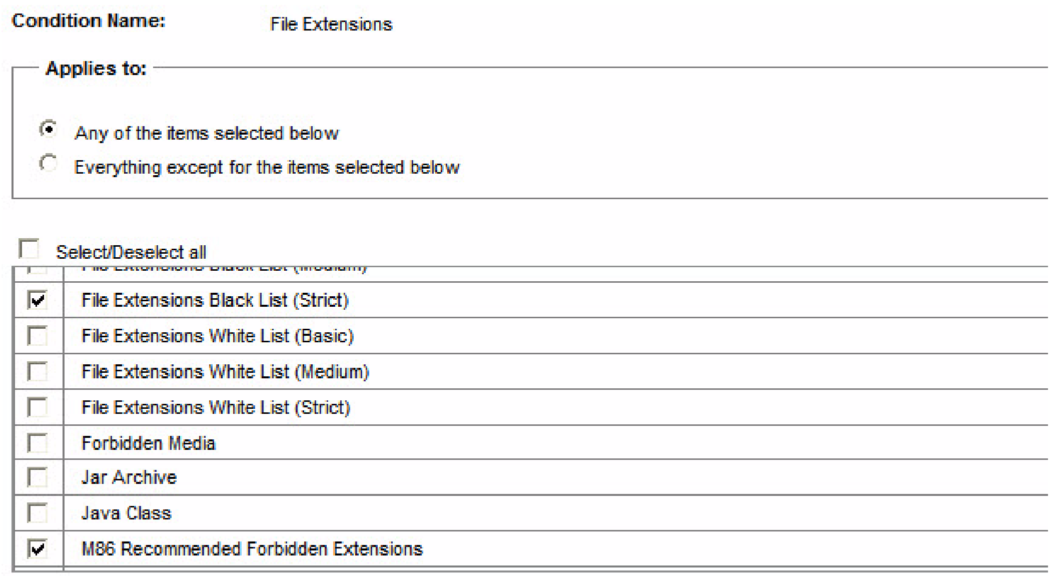
File Extensions
- Web Content
  - JS
- Multiple Extensions
  - Multiple Extensions

URL Filtering (IBM)

Figure 3-65: Request: Multiple Extensions

Block Blacklisted File Extensions

The **Block Blacklisted File Extensions** rule blocks file types which may be a security hazard and are not normally used by legitimate sites/applications.



Condition Name: File Extensions

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□ File Extensions Black List (Medium)

☑ File Extensions Black List (Strict)

□ File Extensions White List (Basic)

□ File Extensions White List (Medium)

□ File Extensions White List (Strict)

□ Forbidden Media

□ Jar Archive

□ Java Class

☑ M86 Recommended Forbidden Extensions

Figure 3-66: Block Blacklisted File Extensions

The following table displays the Rule Editor definitions:

Block Blacklisted File Extensions	
Action	Block
End-User Message	File Extension
Conditions	
File Extension	M86 Recommended Forbidden Extensions, Block File Extensions (Strict/Medium)

Further information:

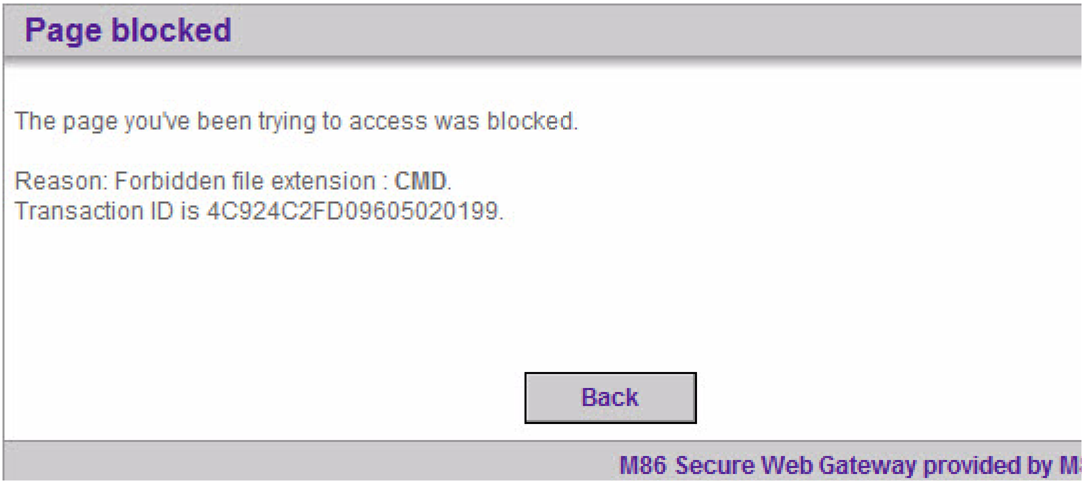
- M86 Recommended Forbidden Extensions cannot be edited by the administrator. However, it can be viewed at **Policies → Condition Settings →File extensions**.

Rule Demonstration:

➲ To test the Block Blacklisted File Extensions rule:

1. Copy and paste the following URL into your browser: http://www.m86security.com/EVG/dir.cmd
2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



Page blocked

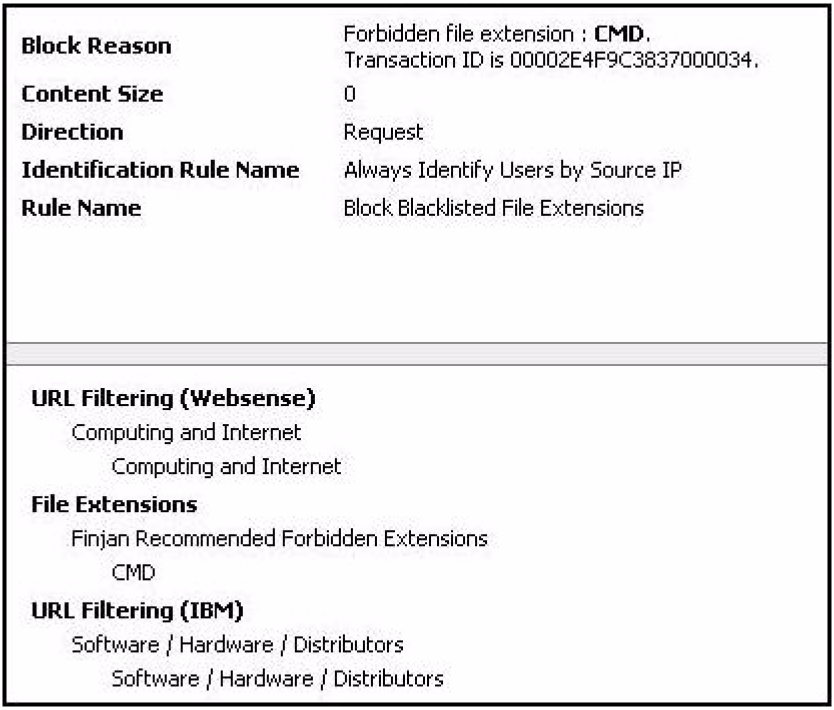
The page you've been trying to access was blocked.

Reason: Forbidden file extension : CMD.
Transaction ID is 4C924C2FD09605020199.

Figure 3-67: Page Blocked - Forbidden File Extensions

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click ☰ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request** to obtain further information on the Request phase of this transaction. Only the

Request component exists for this transaction since it was blocked at the request phase.



Block Reason	Forbidden file extension : **CMD**. Transaction ID is 00002E4F9C3837000034.
Content Size	0
Direction	Request
Identification Rule Name	Always Identify Users by Source IP
Rule Name	Block Blacklisted File Extensions

URL Filtering (Websense)

- Computing and Internet
  - Computing and Internet

File Extensions

- Finjan Recommended Forbidden Extensions
  - CMD

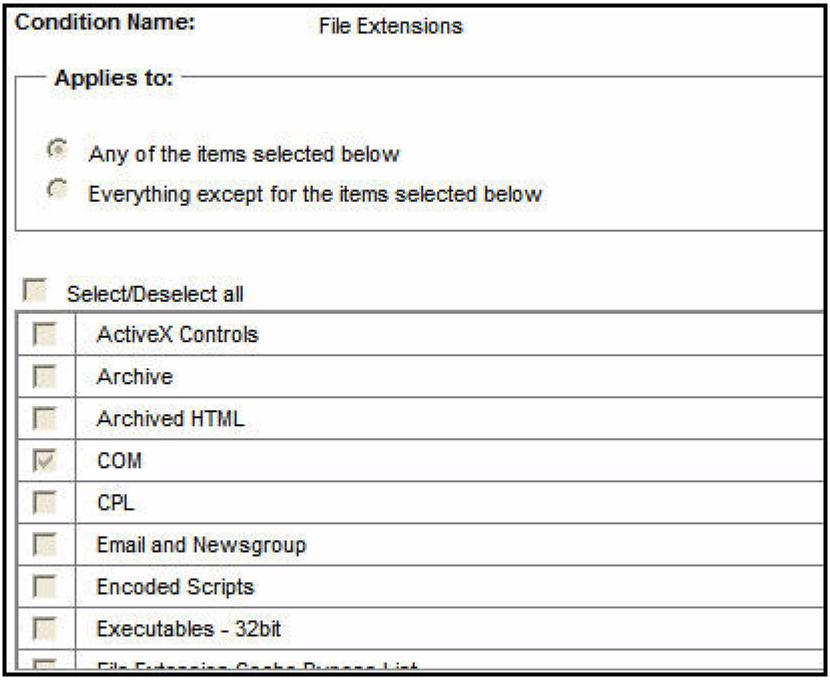
URL Filtering (IBM)

- Software / Hardware / Distributors
  - Software / Hardware / Distributors

Figure 3-68: Request - Forbidden File Extensions

Block Files with COM Extensions

The **Block Files with COM Extensions** rule is designed to block files with com extensions (separately from the **Block Blacklisted File Extensions** rule) which are a known security risk.



Condition Name: File Extensions

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□	ActiveX Controls
□	Archive
□	Archived HTML
☑	COM
□	CPL
□	Email and Newsgroup
□	Encoded Scripts
□	Executables - 32bit
□	File Extension Cache Bypass List

Figure 3-69: Block Files with COM Extensions

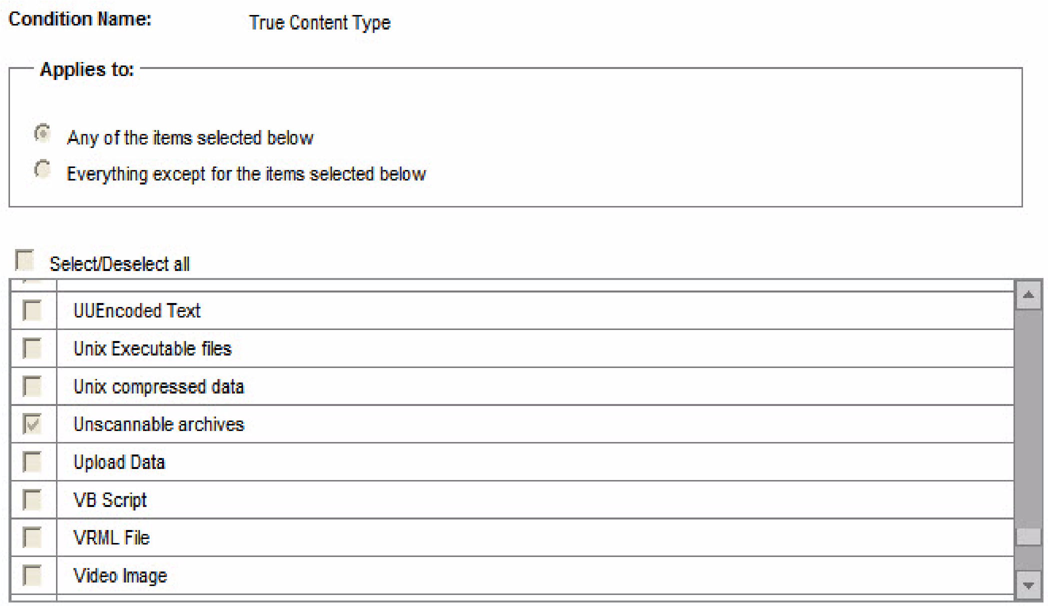
The following table displays the definitions:

Block Files with COM Extensions	
Action	Block
End-User Message	File Extensions
Conditions	
Direction	Incoming
File Extensions	COM
True Content Type	DOS Executable File, Unscannable Data

Block Unscannable Archives

The **Block Unscannable Archives rule** block archives which cannot be opened by M86's engine. Such archives are blocked since there is no risk estimation regarding their content.

NOTES: *This rule is activated before Anti-Virus scanning to protect the Anti-Virus from potential archive viruses contained in such archives*



Condition Name: True Content Type

Applies to:

- ● Any of the items selected below
- ○ Everything except for the items selected below

□ Select/Deselect all

- □ UUEncoded Text
- □ Unix Executable files
- □ Unix compressed data
- ☑ Unscannable archives
- □ Upload Data
- □ VB Script
- □ VRML File
- □ Video Image

Figure 3-70: Block Unscannable Archives

The following table displays the definitions:

Block Unscannable Archives	
Action	Block
End-User Message	Type Detector

Block Unscannable Archives	
Conditions	
True Content Type	Unscannable Archives

Further Information:

- This rule is evaluated at the Response phase.

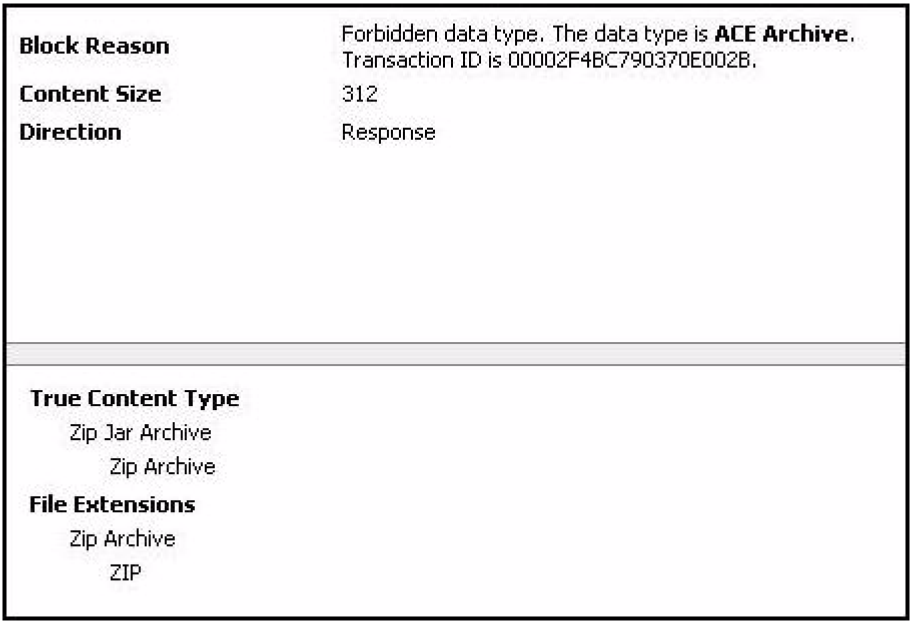
Rule Demonstration:

➲ To test the Block Unscannable Archives rule:

1. Copy and paste the following URL into your browser: http://www.m86security.com/EVG/unaceVulnerability.zip

This URL contains a Zip file with ACE files designed to test ACE’s vulnerabilities.

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.
3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction. The first part of the Response component is a zip file.



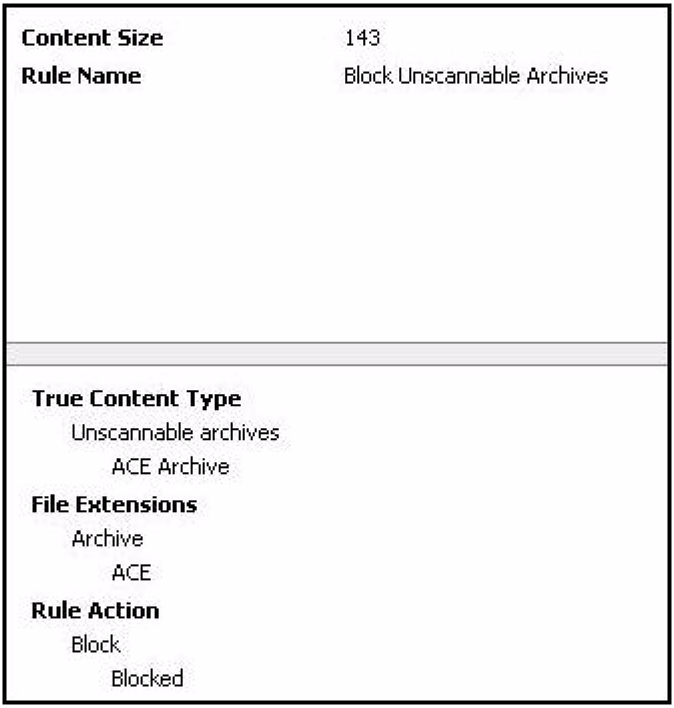
Block Reason	Forbidden data type. The data type is **ACE Archive**. Transaction ID is 00002F4BC790370E002B.
Content Size	312
Direction	Response

True Content Type
- Zip Jar Archive
  - Zip Archive

File Extensions
- Zip Archive
  - ZIP

Figure 3-71: Response 1: Unscannable Archives

6. Click to reveal the second page of the response. You will see that the zip file contains an ACE file and therefore was blocked.



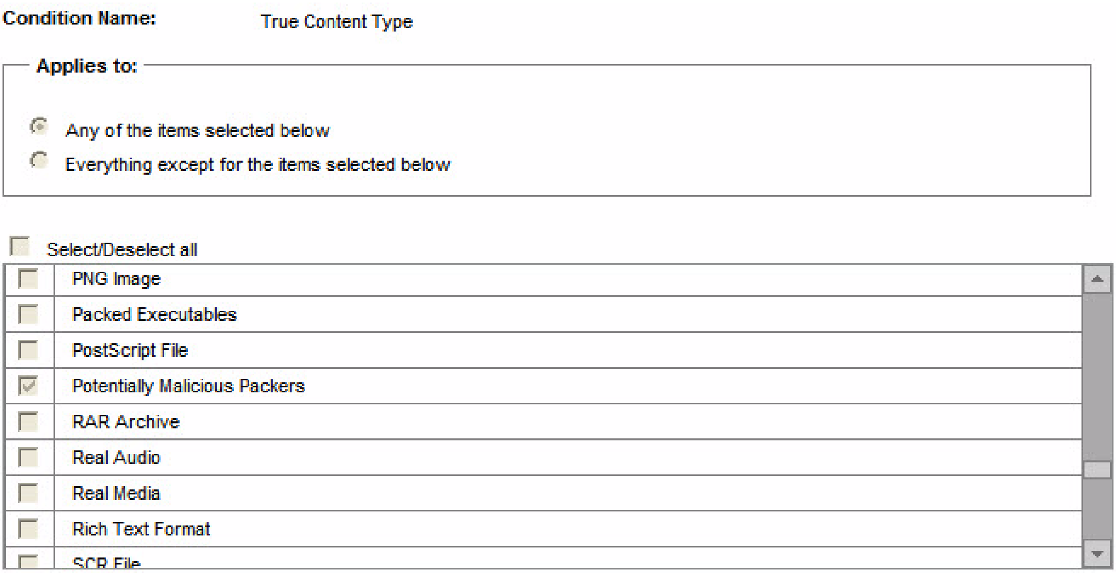
Content Size 143
Rule Name Block Unscannable Archives

True Content Type
Unscannable archives
ACE Archive
File Extensions
Archive
ACE
Rule Action
Block
Blocked

Figure 3-72: Response 2: Unscannable Archives

Block Potentially Malicious Packed Executables

The **Block Potentially Malicious Packed Executables** rule blocks known problematic packed executables which may be used to hide malicious content.



Condition Name: True Content Type

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□	PNG Image
□	Packed Executables
□	PostScript File
☑	Potentially Malicious Packers
□	RAR Archive
□	Real Audio
□	Real Media
□	Rich Text Format
□	SCR File

Figure 3-73: Block Potentially Malicious Packed Executables

The following table displays the definitions:

Block Potentially Malicious Packed Executable	
Action	Block
End-User Message	Type Detector
Conditions	
True Content Type	Potentially Malicious Packers

Further Information:

You must enable one of the Anti-Virus engines (Sophos/McAfee/Kaspersky) in order to use this **Block Potentially Malicious Packed Executables** rule.

Rule Demonstration

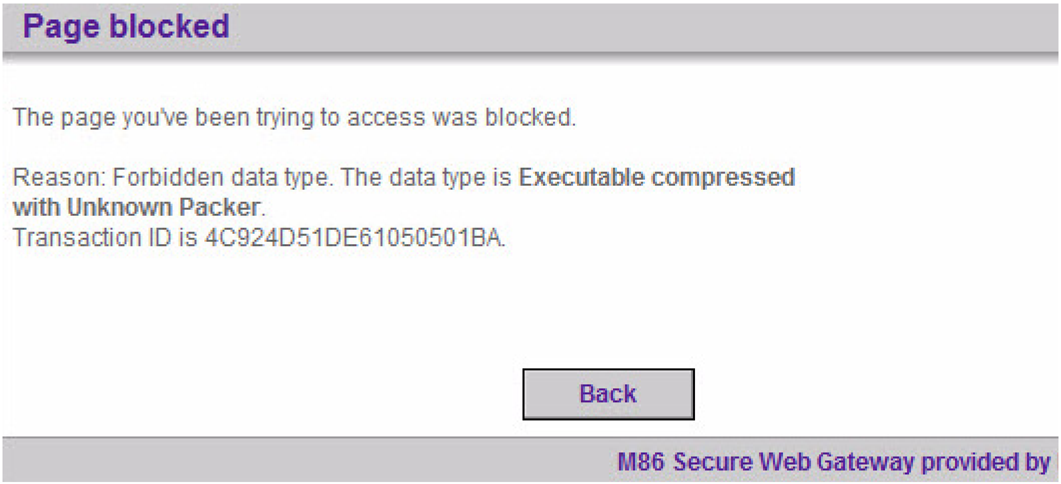
➲ **To test the Block Potentially Malicious Packed Executables rule:**

1. Copy and paste the following URL into your browser:

http://www.m86security.com/EVG/packer.exe

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following message appears:



Page blocked

The page you've been trying to access was blocked.

Reason: Forbidden data type. The data type is **Executable compressed with Unknown Packer**.
Transaction ID is 4C924D51DE61050501BA.

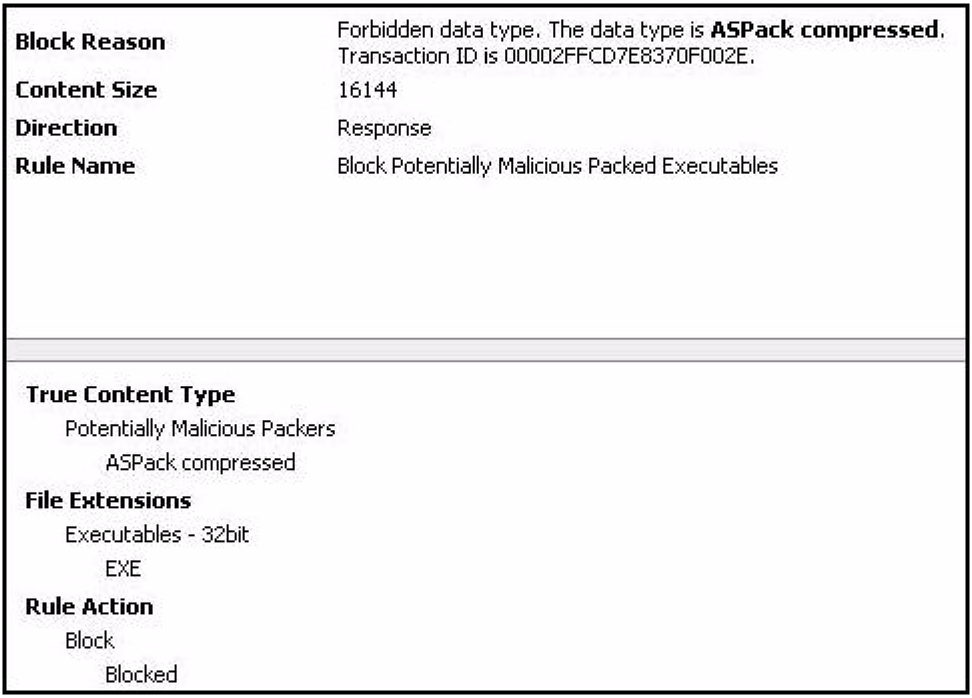
M86 Secure Web Gateway provided by

Figure 3-74: Page Blocked - Packed Executables

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



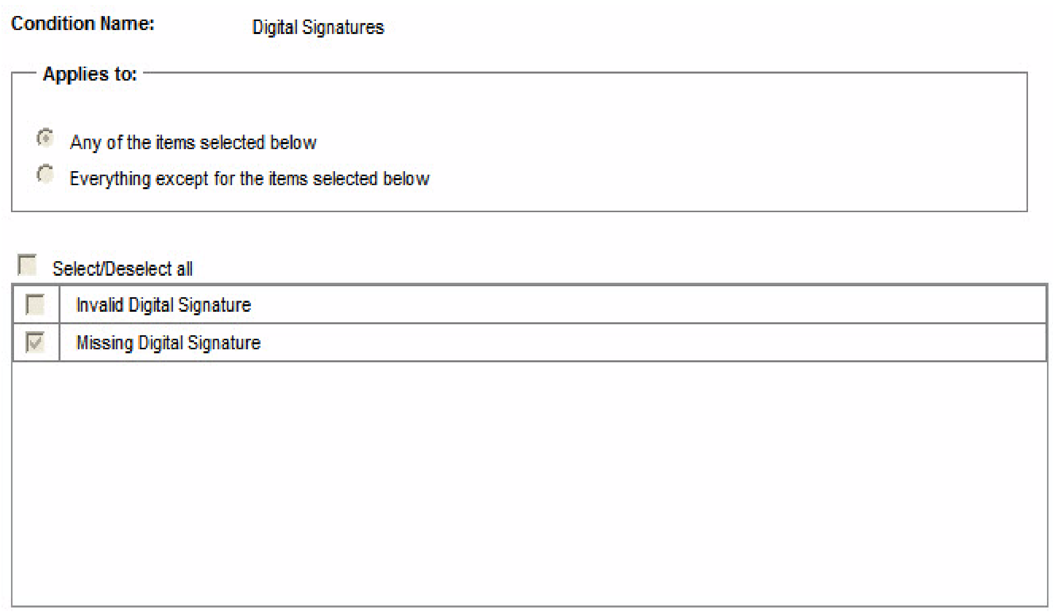
Block Reason	Forbidden data type. The data type is **ASPack compressed**. Transaction ID is 00002FFCD7E8370F002E.
Content Size	16144
Direction	Response
Rule Name	Block Potentially Malicious Packed Executables

True Content Type
Potentially Malicious Packers
ASPack compressed
File Extensions
Executables - 32bit
EXE
Rule Action
Block
Blocked

Figure 3-75: Response: Packed Executables

Block Binary Objects without a Digital Certificate

The **Block Binary Objects without a Digital Certificate** rule blocks binary objects that do not have a digital certificate verifying their integrity. The digital certificate contains information as to who the certificate was issued to and the certifying authority that issued it.



Condition Name: Digital Signatures

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

□	Invalid Digital Signature
☑	Missing Digital Signature

Figure 3-76: Block Binary Objects without a Digital Certificate

The following table displays the Rule Editor definitions:

Block Binary Objects without a Digital Certificate	
Action	Block
End-User Message	Digital Signature Violation
Conditions	
Digital Signatures	Missing Digital Signature

Rule Demonstration

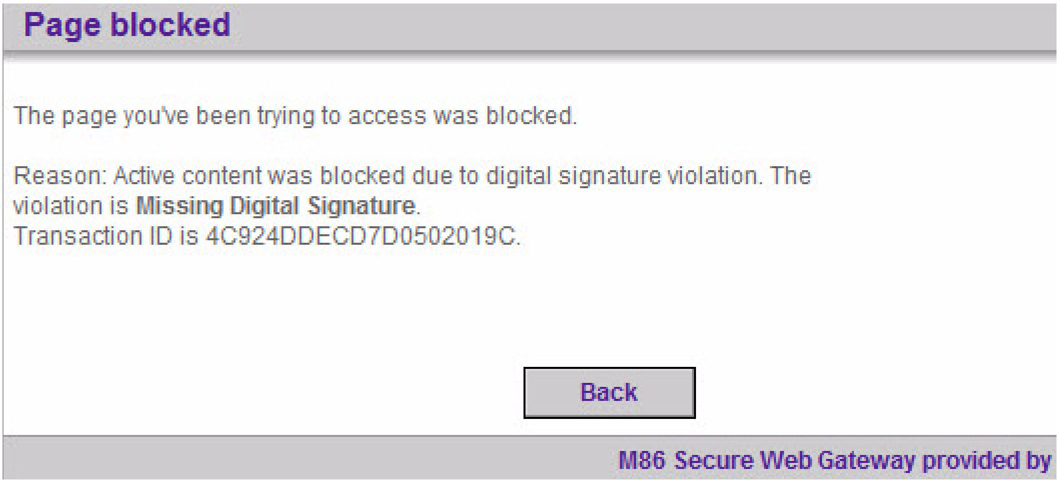
➲ **To test the Block Binary Objects without a Digital Certificate rule:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/no_digital_signature.exe

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following message appears:



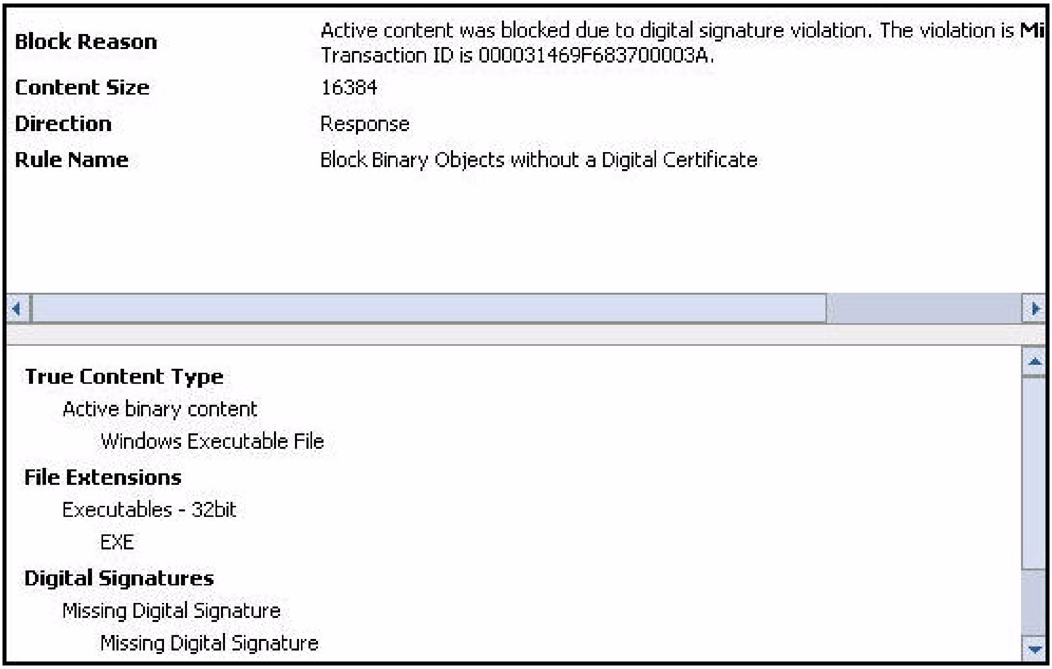
Page blocked

The page you've been trying to access was blocked.

Reason: Active content was blocked due to digital signature violation. The violation is **Missing Digital Signature**.
Transaction ID is 4C924DDECD7D0502019C.

Figure 3-77: Page Blocked - Missing Digital Signature

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click ▸☰ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	Active content was blocked due to digital signature violation. The violation is **Mi** Transaction ID is 000031469F683700003A.
Content Size	16384
Direction	Response
Rule Name	Block Binary Objects without a Digital Certificate

True Content Type
- Active binary content
  - Windows Executable File

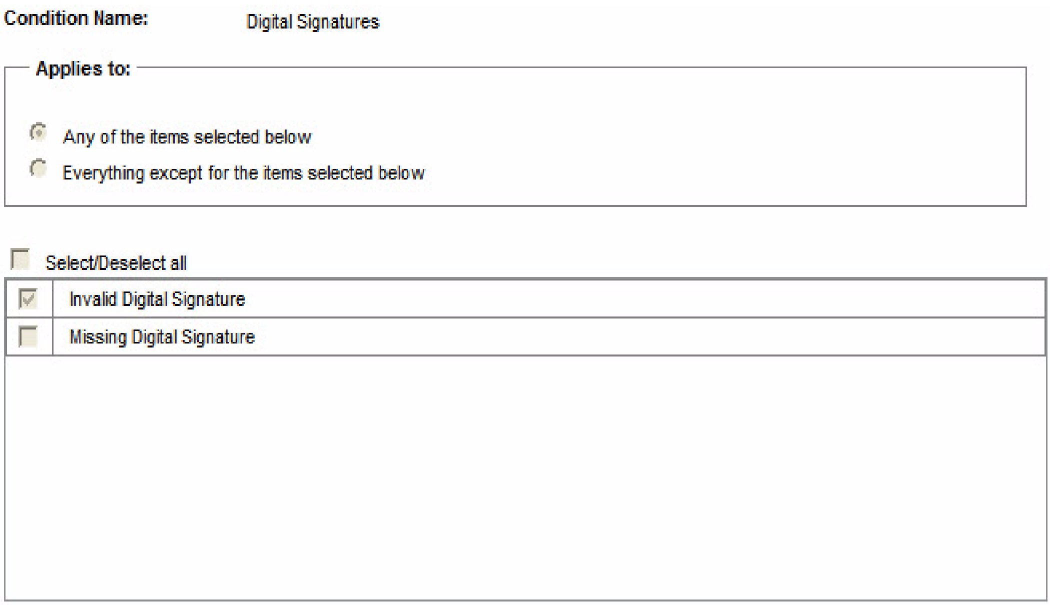
File Extensions
- Executables - 32bit
  - EXE

Digital Signatures
- Missing Digital Signature
  - Missing Digital Signature

Figure 3-78: Response: Missing Digital Signature

Block Binary Objects with Invalid Digital Certificate

The **Block Binary Objects with Invalid Digital Certificate** rule blocks binary objects which, for various reasons, have an incorrect Digital Certificate attached.



Condition Name: Digital Signatures

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

☑	Invalid Digital Signature
□	Missing Digital Signature

Figure 3-79: Block Binary Objects with Invalid Digital Certificate

The following table displays the definitions:

Block Binary Objects with Invalid Digital Certificate	
Action	Block
End-User Message	Digital Signature Violation
Conditions	
Digital Signatures	Invalid Digital Signature

Rule Demonstration

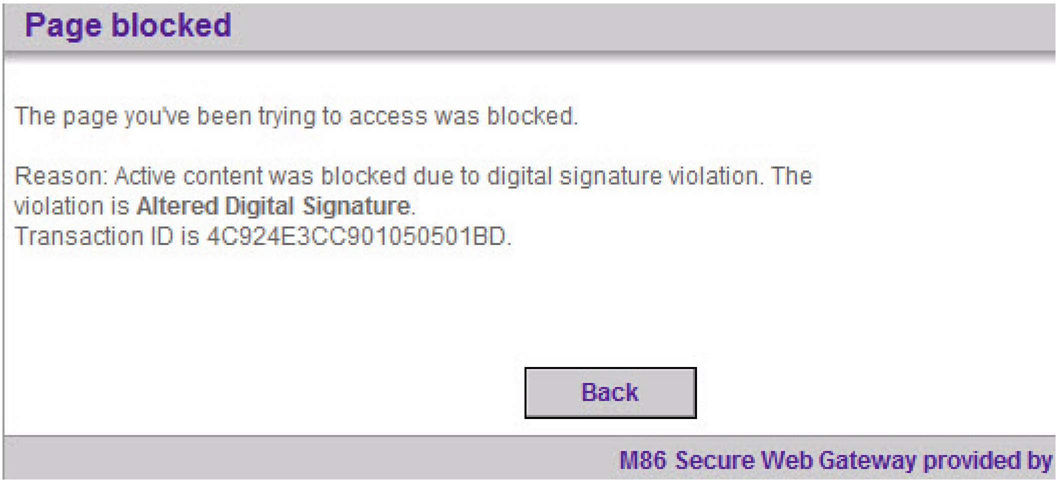
➲ **To test the Block Binary Objects with Invalid Digital Certificate rule:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/invalid%20signature.exe

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following message appears:



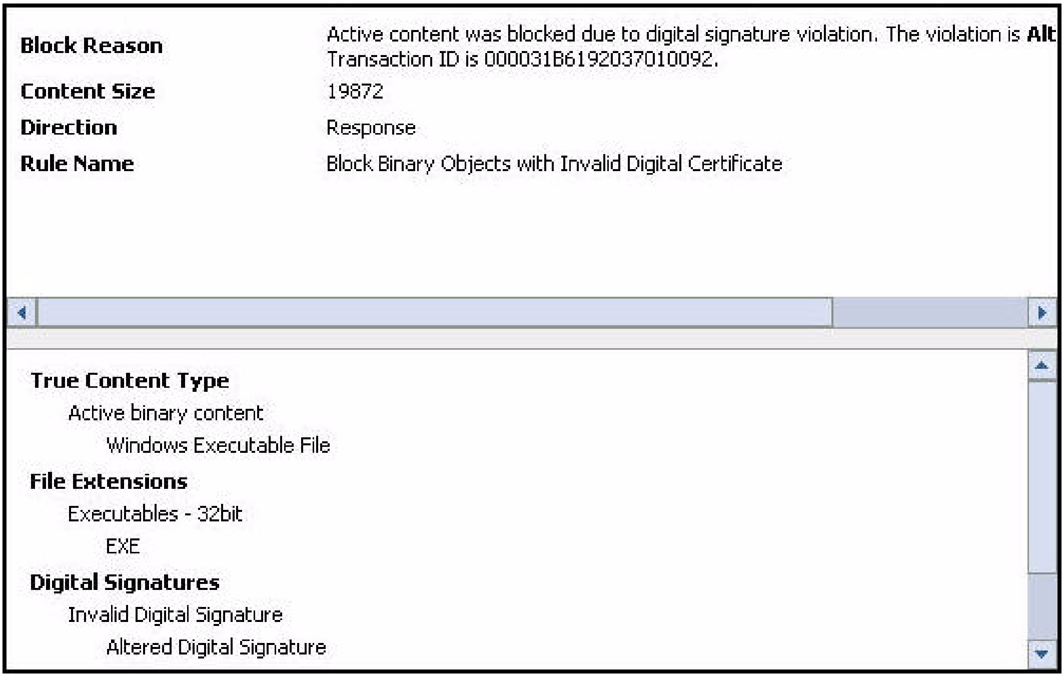
Page blocked

The page you've been trying to access was blocked.

Reason: Active content was blocked due to digital signature violation. The violation is **Altered Digital Signature**.
Transaction ID is 4C924E3CC901050501BD.

Figure 3-80: Page Blocked - Invalid Signature

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	Active content was blocked due to digital signature violation. The violation is **Alt** Transaction ID is 000031B6192037010092.
Content Size	19872
Direction	Response
Rule Name	Block Binary Objects with Invalid Digital Certificate

True Content Type
- Active binary content
  - Windows Executable File

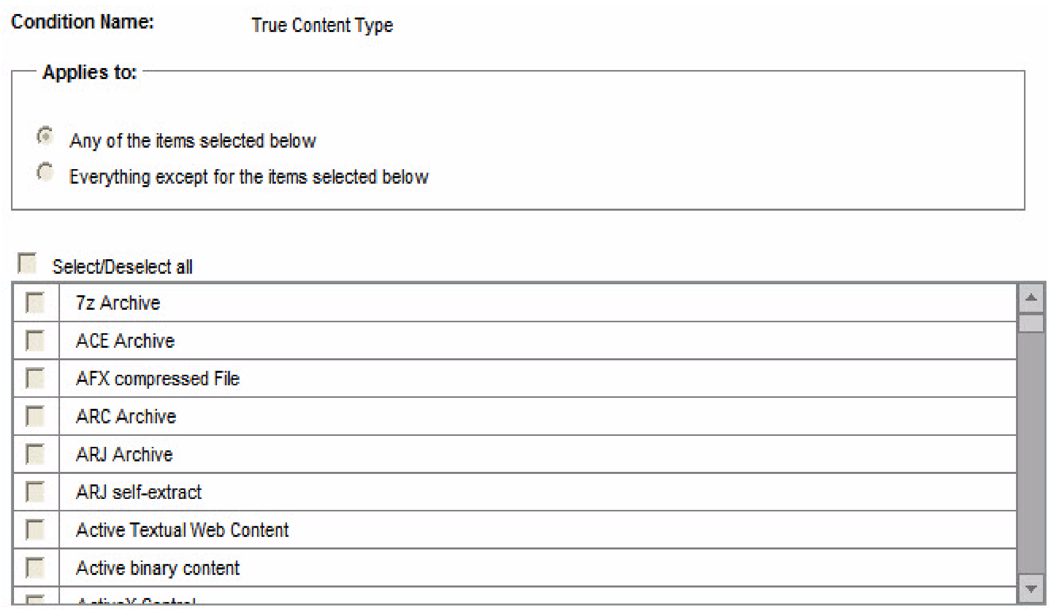
File Extensions
- Executables - 32bit
  - EXE

Digital Signatures
- Invalid Digital Signature
  - Altered Digital Signature

Figure 3-81: Response: Invalid Digital Signature

Block Customer-Defined True Content Type

The **Block Customer-Defined True Content Type** rule rule only appears in the M86 Basic Security Policy and will contain the content type that you chose through the Simplified Setup interface.



Condition Name: True Content Type

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□ 7z Archive

□ ACE Archive

□ AFX compressed File

□ ARC Archive

□ ARJ Archive

□ ARJ self-extract

□ Active Textual Web Content

□ Active binary content

□ ActiveX Control

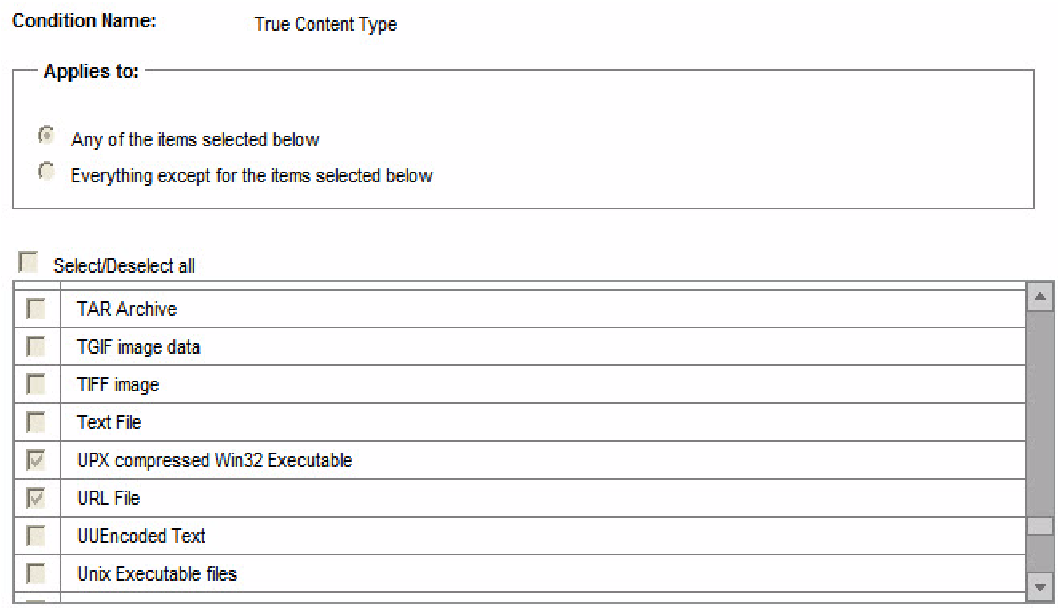
Figure 3-82: Block Customer-Defined True Content Type

The following table displays the definitions:

Block Customer-Defined True Content Type	
Action	Block
End-User Message	Suspicious File Type Detected
Conditions	
True Content Type	Options chosen via the Simplified Setup will be displayed here.

Block Suspicious File Types

The **Block Suspicious File Types** rule complements the Forbid Blacklisted File Extensions rule by checking the **true type** of the downloaded content and preventing extension spoofing which might have bypassed the Forbid Blacklisted File Extensions rule.



Condition Name: True Content Type

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

□	TAR Archive
□	TGIF image data
□	TIFF image
□	Text File
☑	UPX compressed Win32 Executable
☑	URL File
□	UUEncoded Text
□	Unix Executable files

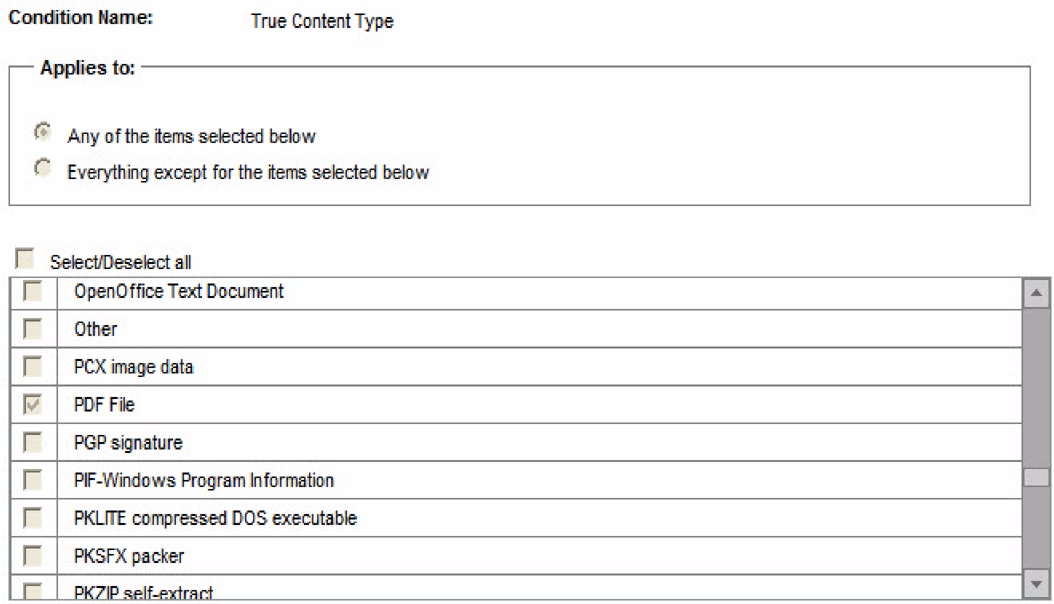
Figure 3-83: Block Suspicious File Types

The following table displays the Rule definitions:

Block Suspicious File Types	
Action	Block
End-User Message	Suspicious File Type Detected
Conditions	
True Content Type	DOS Executable file, Link File, MSI Installation Package, Microsoft Outlook MSG Document, PIF-Windows Program Information, UPX compressed Win32 Executable, URL File, Windows Metafile, Windows registry files

Block Rich Content Application Level Vulnerabilities

The **Block Rich Content Application Level Vulnerabilities** rule uses M86's proprietary engine Vulnerability Anti.dote™ and the Behavior Profile (Scripts) engine. These are unique security engines, designed to identify and block malicious content which tries to exploit known and unknown software vulnerabilities. It is updated regularly by M86's MCRC.



Condition Name: True Content Type

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

□	OpenOffice Text Document
□	Other
□	PCX image data
☑	PDF File
□	PGP signature
□	PIF-Windows Program Information
□	PKLITE compressed DOS executable
□	PKSFX packer
□	PKZIP self-extract

Figure 3-84: Block Rich Content Application Level Vulnerability Rule

The following table displays the Rule Editor definitions

Block Rich Content Application Level Vulnerabilities	
Action	Block
End-User Message	Application Level Vulnerability Detected
Conditions	
Behavior Profile (Scripts)	Vulnerability Anti.dote Profile
Behavior Profile	Default Profile - Script behavior

Further Information:

The **Block Application Level Vulnerabilities** rule refers to the **Vulnerability Anti.dote** Profile which can be found via **Policies → Condition Settings → Vulnerability Anti.dote →Vulnerability Anti.dote Profile**.

This Security Engine consists of vulnerability groups, each of which contains a sub group of vulnerabilities, for example, Crashing Internet Clients.

Rule Demonstration:

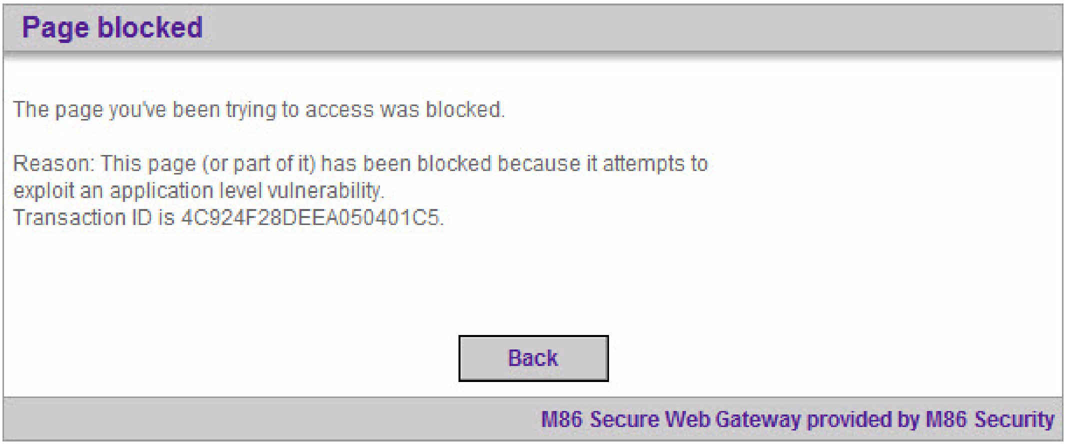
➲ **To test the Behavior Profile rule with a selection of Generic shell code in a Flash or PDF file:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/rds.swf

   This link attempts to open a calculator.
2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**,and click **OK**.

The following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

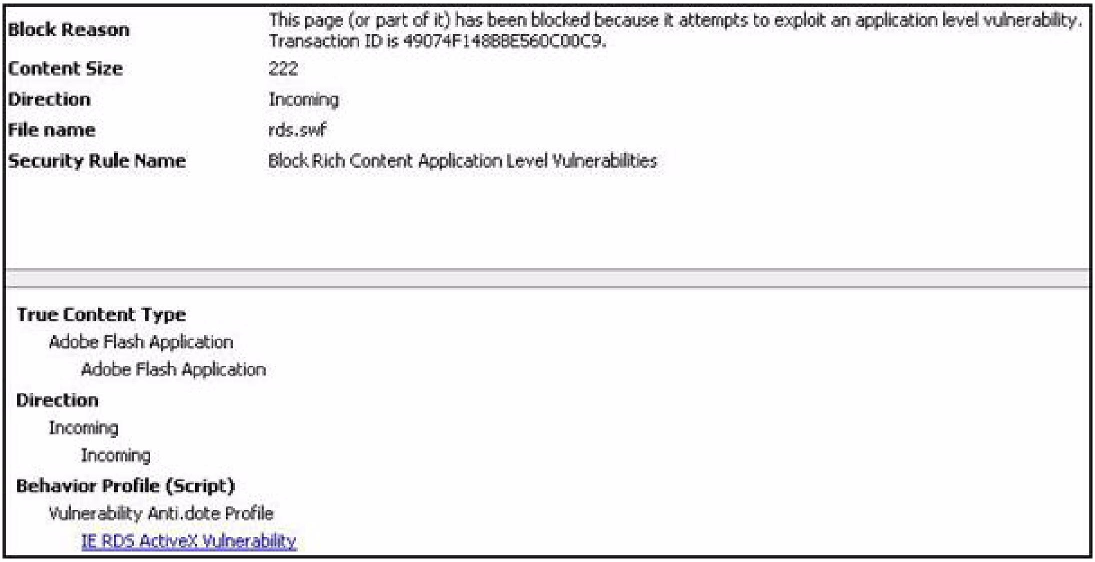
Reason: This page (or part of it) has been blocked because it attempts to exploit an application level vulnerability.
Transaction ID is 4C924F28DEEA050401C5.

Figure 3-85: Page Blocked Rich Content Application Level

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▤ and select **Details**. TheTransaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click Request/Response to obtain further information on the Request and Response phases of this transaction.



Block Reason	This page (or part of it) has been blocked because it attempts to exploit an application level vulnerability. Transaction ID is 49074F148BBE560C00C9.
Content Size	222
Direction	Incoming
File name	rds.swf
Security Rule Name	Block Rich Content Application Level Vulnerabilities

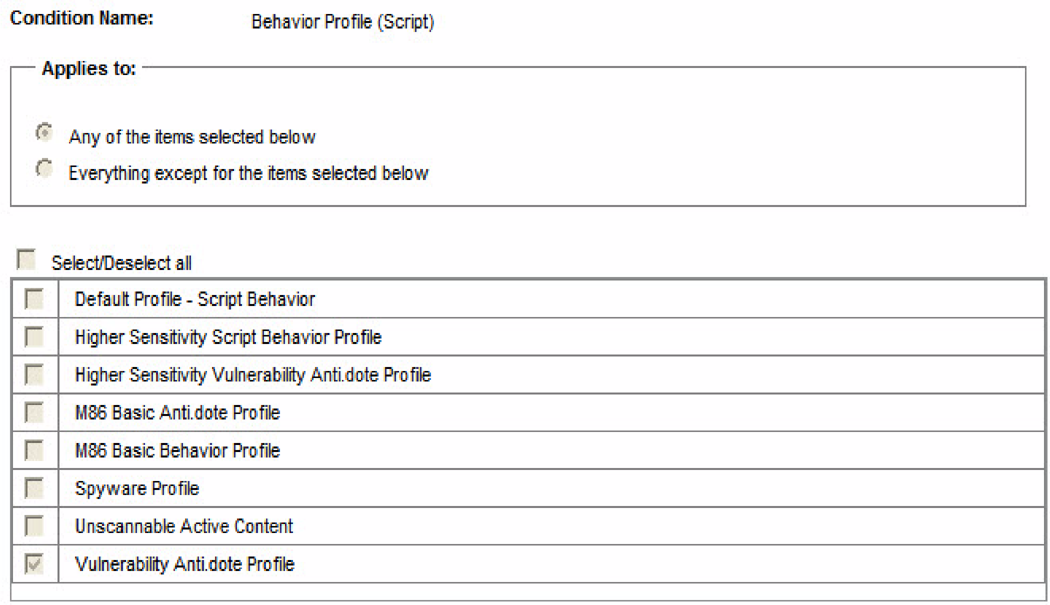
- **True Content Type**
  - Adobe Flash Application
    - Adobe Flash Application
- **Direction**
  - Incoming
    - Incoming
- **Behavior Profile (Script)**
  - Vulnerability Anti.dote Profile
    - IE RDS ActiveX Vulnerability

Figure 3-86: Transaction Details

This page was blocked due to attempts to exploit an application level vulnerability violation.

Block Application Level Vulnerabilities

The **Block Application Level Vulnerabilities** rule uses M86's proprietary engine: Vulnerability Anti.dote™. This is a unique security engine, designed to identify and block malicious content which tries to exploit known software vulnerabilities. It is updated regularly by M86's MCRC.



Condition Name: Behavior Profile (Script)

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□	Default Profile - Script Behavior
□	Higher Sensitivity Script Behavior Profile
□	Higher Sensitivity Vulnerability Anti.dote Profile
□	M86 Basic Anti.dote Profile
□	M86 Basic Behavior Profile
□	Spyware Profile
□	Unscannable Active Content
☑	Vulnerability Anti.dote Profile

Figure 3-87: Block Application Level Vulnerabilities rule

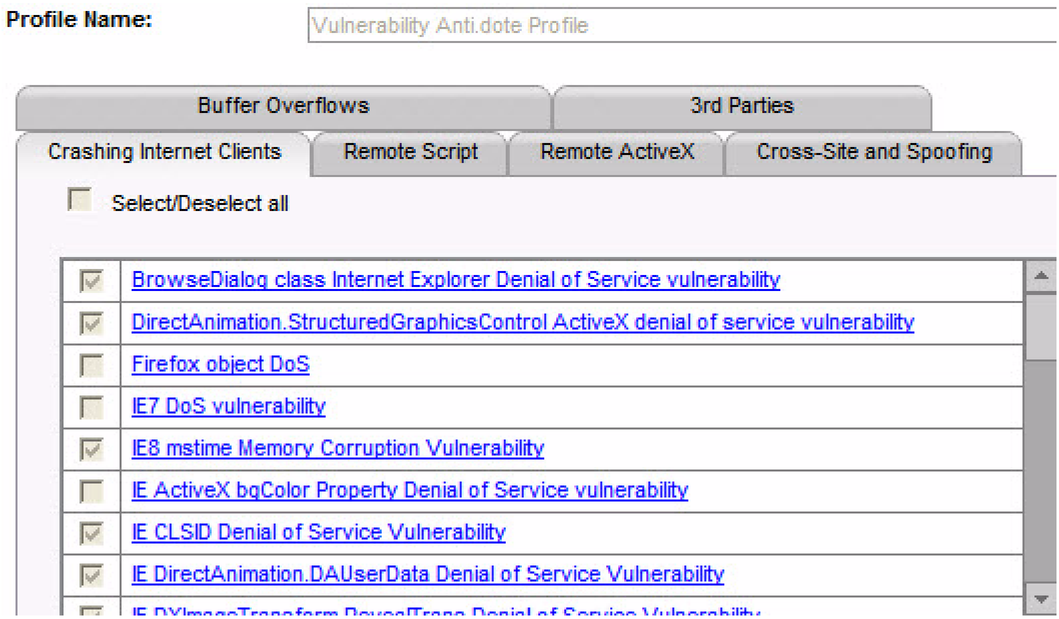
The following table displays the Rule Editor definitions:

Block Application Level Vulnerabilities	
Action	Block
End-User Message	Application Level Vulnerability Detected
Conditions	
Behavior Profile (Scripts)	Vulnerability Anti.dote Profile

Further Information:

The **Block Application Level Vulnerabilities** rule refers to the **Vulnerability Anti.dote** Profile which can be found via **Policies →**

Condition Settings → Vulnerability Anti.dote →Vulnerability Anti.dote Profile.



Profile Name: Vulnerability Anti.dote Profile

□ Select/Deselect all

☑ BrowseDialog class Internet Explorer Denial of Service vulnerability
☑ DirectAnimation.StructuredGraphicsControl ActiveX denial of service vulnerability
□ Firefox object DoS
□ IE7 DoS vulnerability
☑ IE8 mstime Memory Corruption Vulnerability
□ IE ActiveX bgColor Property Denial of Service vulnerability
☑ IE CLSID Denial of Service Vulnerability
☑ IE DirectAnimation.DAUserData Denial of Service Vulnerability
☑ IE DXImageTransform.RevealTrans Denial of Service Vulnerability

Figure 3-88: Vulnerability Anti.dote Profile

This Security Engine consist of vulnerability groups, each of which contains a sub group of vulnerabilities, for example, Crashing Internet clients.

Rule Demonstration:

This section focuses on sub-groups of the Vulnerability Anti.dote Profile.

Crashing Internet clients Sub group (Browser, IM, etc)

The **Crashing Internet Clients (Browser, IM, etc)** sub-group defines a set of vulnerabilities which may cause a denial of service (DOS).

In this example, the rule is tested with selection of the IE

TriEditDocument Denial of Service Vulnerability.

Example One:

➲ **To test the Block Application Level Vulnerabilities rule with selection of the Crashing Internet Clients > IE TriEditDocumentDenial of Service Vulnerability:**

1. Copy and paste the following URL into your browser:

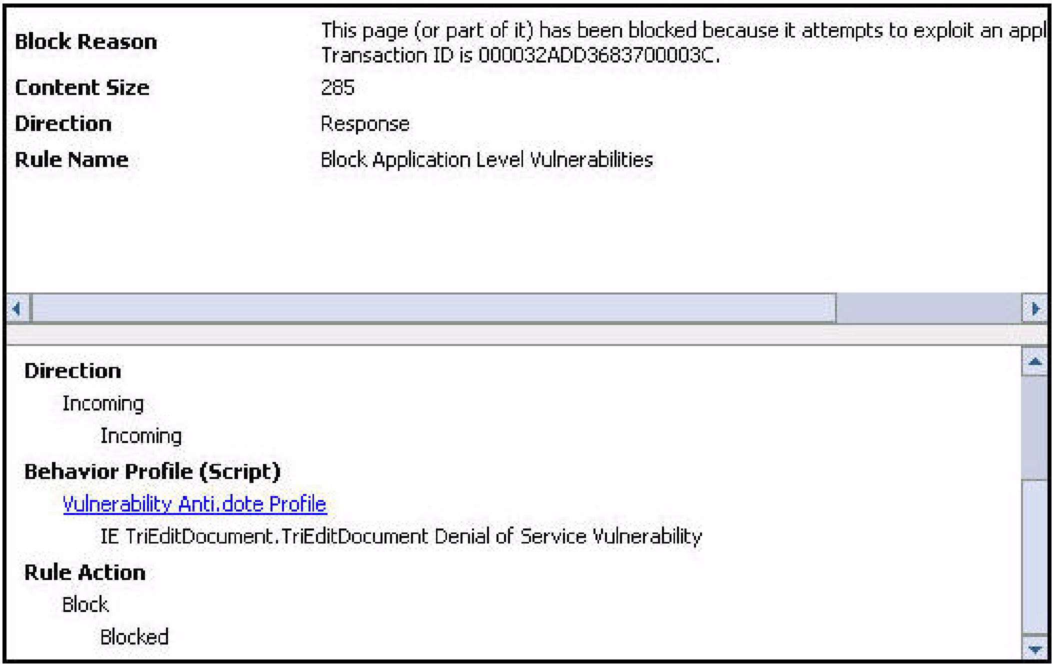
   http://www.m86security.com/EVG/testdemo.htm

   This site exploits a vulnerability of Internet Explorer that will cause it to crash.

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click 📋 and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason This page (or part of it) has been blocked because it attempts to exploit an appl
Transaction ID is 000032ADD3683700003C.

Content Size 285

Direction Response

Rule Name Block Application Level Vulnerabilities

Direction
Incoming
Incoming

Behavior Profile (Script)
Vulnerability Anti.dote Profile
IE TriEditDocument.TriEditDocument Denial of Service Vulnerability

Rule Action
Block
Blocked

Figure 3-89: Response: Vulnerabilities - Crashing Internet Clients

As can be seen in the **Response** window, the page was blocked due to detection of **IE TriEditDocument Denial of Service Vulnerability**, which is a sub-section of the Crashing Internet Client group.

Script Remote Code Execution – Cross zone scripting:

Script remote code execution group refers to vulnerabilities which enable the attacker to execute code on a remote machine by elevation of the page security zone.

Example One:

➲ **To test the Block Application Level Vulnerabilities rule with selection of the Script Remote code execution:**

1. Copy and paste the following URL into your browser:

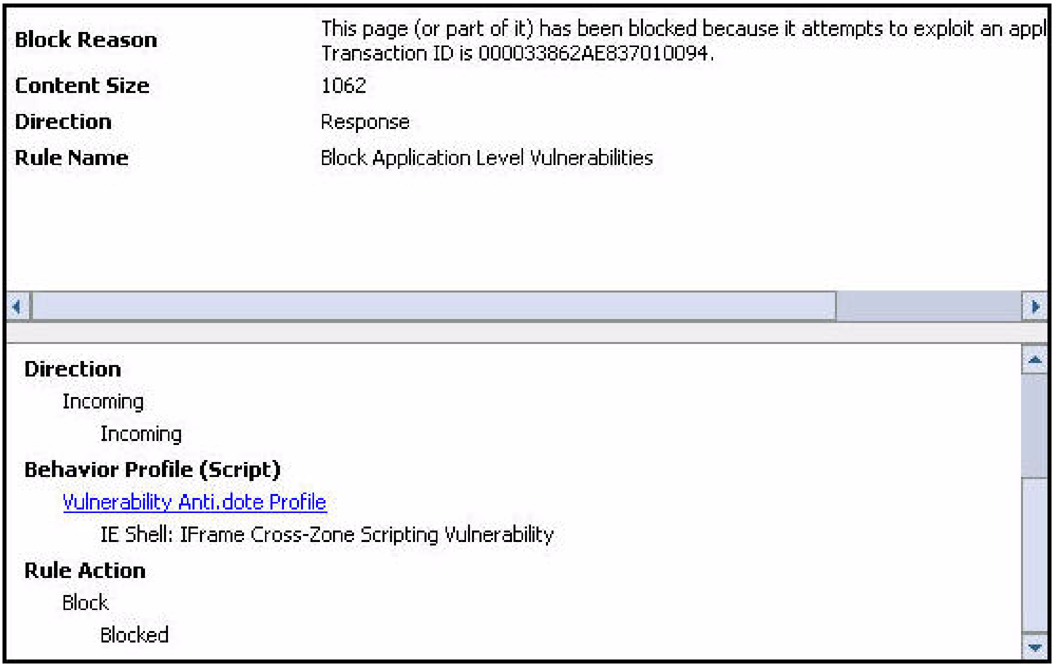
http://www.m86security.com/EVG/9628.html

This link tries to open port (28876) by exploiting MSIE DHTML Object handling vulnerabilities:

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	This page (or part of it) has been blocked because it attempts to exploit an appl Transaction ID is 000033862AE837010094.
Content Size	1062
Direction	Response
Rule Name	Block Application Level Vulnerabilities

Direction
Incoming
Incoming
Behavior Profile (Script)
Vulnerability Anti.dote Profile
IE Shell: IFrame Cross-Zone Scripting Vulnerability
Rule Action
Block
Blocked

Figure 3-90: Response- Script Remote code execution

As can be seen in the **Response** screen, this page was blocked due to detection of **IE Shell: IFrame Cross-Zone Scripting Vulnerability.**

Example Two:

➲ **To test the Block Application Level Vulnerabilities rule with selection of the Script Remote code execution:**

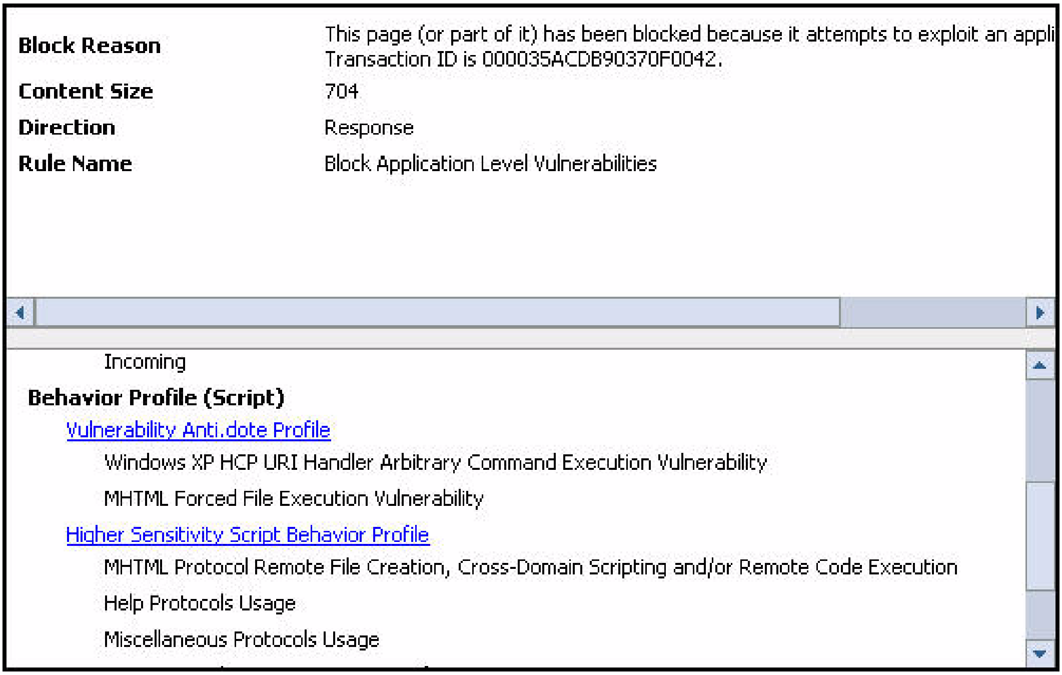
1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/mmulti.htm

   This page tries to exploit multiple vulnerabilities in IE in order to write and execute c:\browsercheck.exe.

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	This page (or part of it) has been blocked because it attempts to exploit an appli Transaction ID is 000035ACDB90370F0042.
Content Size	704
Direction	Response
Rule Name	Block Application Level Vulnerabilities

Incoming

Behavior Profile (Script)

Vulnerability Anti.dote Profile

Windows XP HCP URI Handler Arbitrary Command Execution Vulnerability

MHTML Forced File Execution Vulnerability

Higher Sensitivity Script Behavior Profile

MHTML Protocol Remote File Creation, Cross-Domain Scripting and/or Remote Code Execution

Help Protocols Usage

Miscellaneous Protocols Usage

Figure 3-91: Response: Vulnerabilities- Script Remote code execution

As can be seen in the **Response** window the page was blocked due to multiple violations of browser vulnerabilities and malicious behavior detection.

This page eludes the Anti-Virus scanners by adding multiple \0 (null bytes) to a well known exploitation. This demonstrates the weakness of the traditional Anti-Virus engine with small changes, even in well known exploitations.

Remote code execution via System ActiveX Controls

This group refers to vulnerabilities in the System ActiveX Controls through which an attacker can execute code on an unprotected remote machine.

Example:

➲ **To test the Block Application Level Vulnerabilities rule with selection of the Remote code execution via System Active X Controls:**

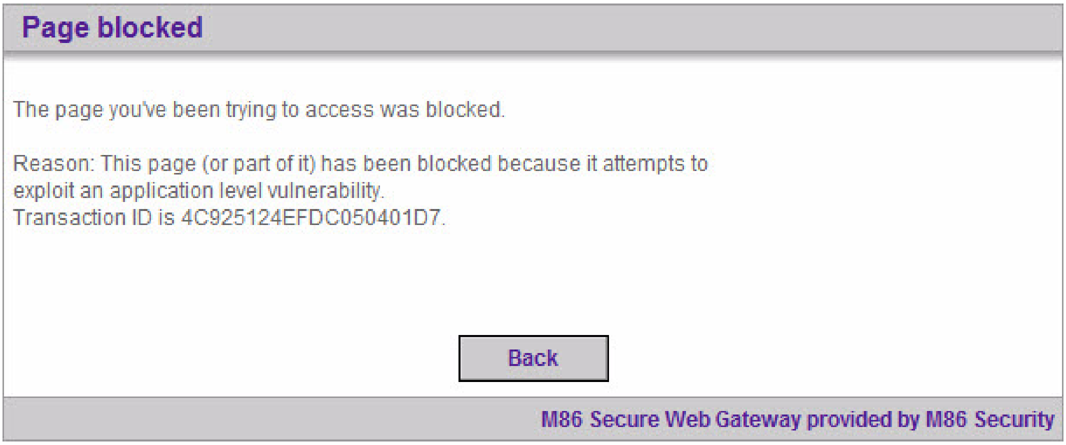
1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/malware.zip

   This link will download and execute code on an unpatched machine exploiting a vulnerability of Windows Media Player.

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

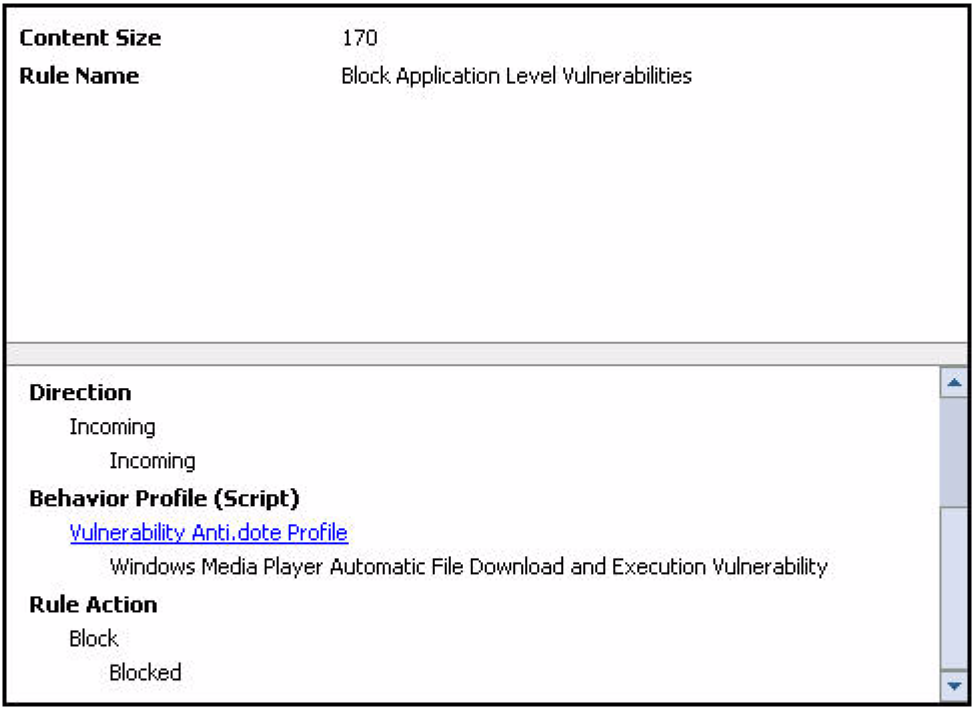
Reason: This page (or part of it) has been blocked because it attempts to exploit an application level vulnerability.
Transaction ID is 4C925124EFDC050401D7.

Figure 3-92: Page Blocked: Vulnerabilities - System ActiveX Controls

3. Return to the Management Console and select the **Logs →** **View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▶≡ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Content Size	170
Rule Name	Block Application Level Vulnerabilities

Direction

Incoming

Incoming

Behavior Profile (Script)

Vulnerability Anti.dote Profile

Windows Media Player Automatic File Download and Execution Vulnerability

Rule Action

Block

Blocked

Figure 3-93: Response: Vulnerabilities - System ActiveX Controls

As can be seen in the **Response** screen, this page was blocked due to detection of **Windows Media Player Automatic File Download and Execution Vulnerability** exploitation.

Cross Site Scripting and Spoofing Vulnerabilities:

This vulnerabilities group refers to vulnerabilities which allow an attacker to insert malicious code into a web-based application (XSS) or any other technique which may result in data compromise.

Example:

➲ To test the Block Application Level Vulnerabilities rule with selection of the Cross Site Scripting and Spoofing Vulnerabilities:

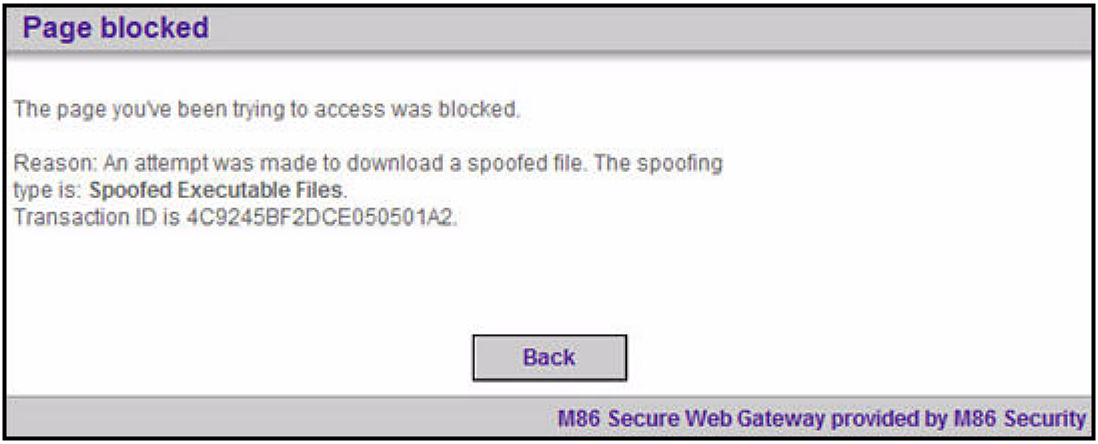
1. Copy and paste the following URL into your browser

   http://www.m86security.com/EVG/clipy.htm

   This link exploits a vulnerability which can steal the user's clipboard.

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

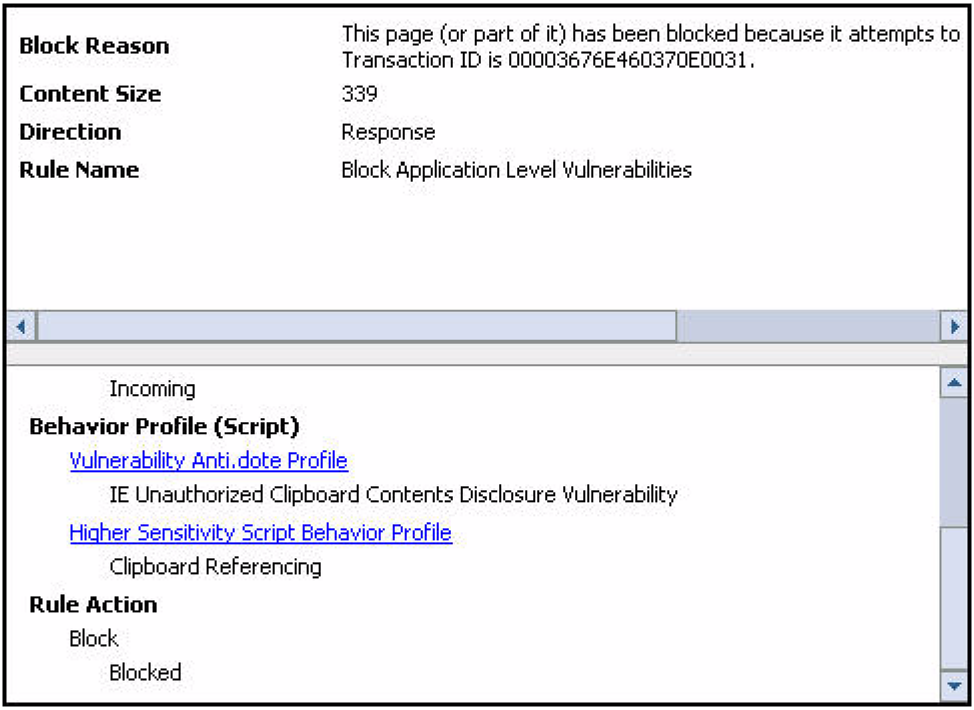
Reason: An attempt was made to download a spoofed file. The spoofing type is: Spoofed Executable Files.
Transaction ID is 4C9245BF2DCE050501A2.

Figure 3-94: Page Blocked: Vulnerabilities: Cross Site Scripting and Spoofing

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason This page (or part of it) has been blocked because it attempts to Transaction ID is 00003676E460370E0031.

Content Size 339

Direction Response

Rule Name Block Application Level Vulnerabilities

Incoming

Behavior Profile (Script)

Vulnerability Anti.dote Profile

IE Unauthorized Clipboard Contents Disclosure Vulnerability

Higher Sensitivity Script Behavior Profile

Clipboard Referencing

Rule Action

Block

Blocked

Figure 3-95: Response: Vulnerabilities- Cross-Site Scripting and Spoofing

As can be seen in the Response screen, this page was blocked due to detection of **IE Unauthorized Clipboard Contents Disclosure Vulnerability** exploit.

Exploitable Buffer Overflows (shell code/create process):

This sub-group refers to vulnerabilities which enable an attacker to execute code on a remote machine by causing a buffer overflow.

Example:

➲ To test the Block Application Level Vulnerabilities rule with selection of the Exploitable Buffer Overflows:

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/createtextrange.html

   This page tries to exploit a vulnerability in IE through which a code execution can be triggered by causing a buffer overflow.

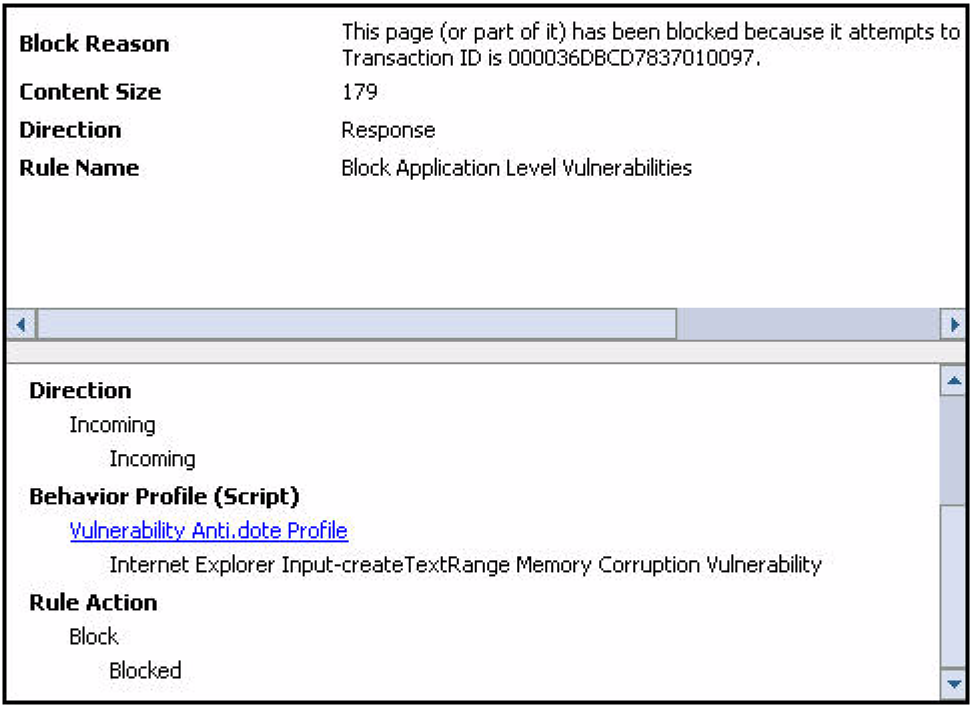
2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	This page (or part of it) has been blocked because it attempts to Transaction ID is 000036DBCD7837010097.
Content Size	179
Direction	Response
Rule Name	Block Application Level Vulnerabilities

Direction
- Incoming
  - Incoming

Behavior Profile (Script)
- Vulnerability Anti.dote Profile
  - Internet Explorer Input-createTextRange Memory Corruption Vulnerability

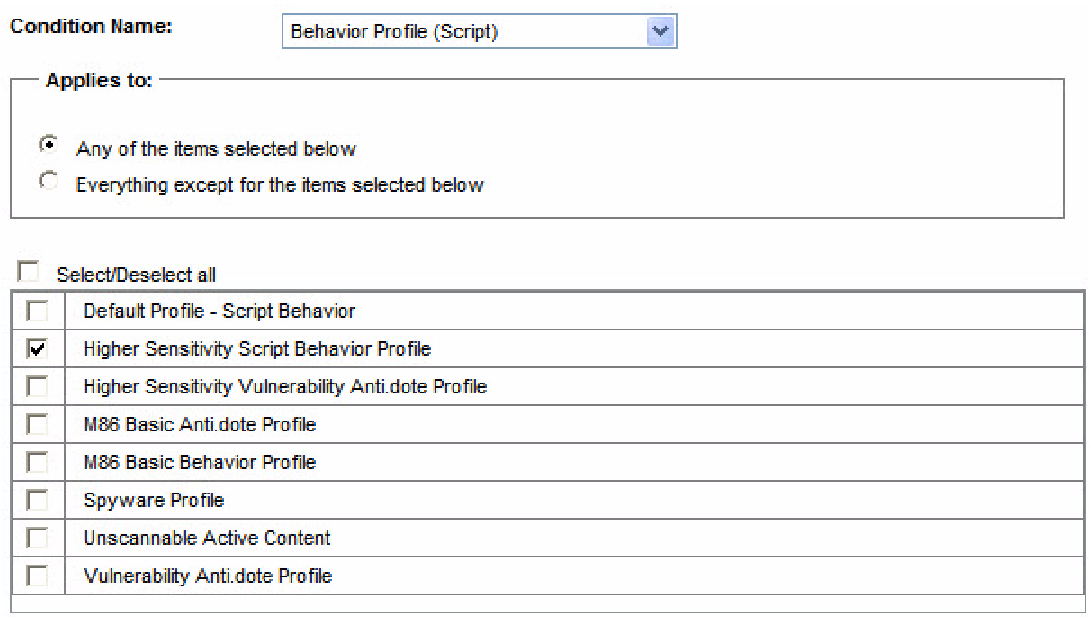
Rule Action
- Block
  - Blocked

Figure 3-96: Response: Vulnerabilities –Exploitable Buffer Overflows

As can be seen in the Response screen, this page was blocked due to detection of **Internet Explorer Input-create TextRange Memory Corruption Vulnerability**.

Block Malicious Scripts by Behavior

The **Block Malicious Scripts by Behavior** rule uses the M86 proprietary Behavior Profile (Scripts) engine. This is a unique security engine, designed to identify and block malicious content by identifying combinations of operations, parameters, script manipulations and other exploitation techniques for a given piece of content.



Condition Name: Behavior Profile (Script)

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

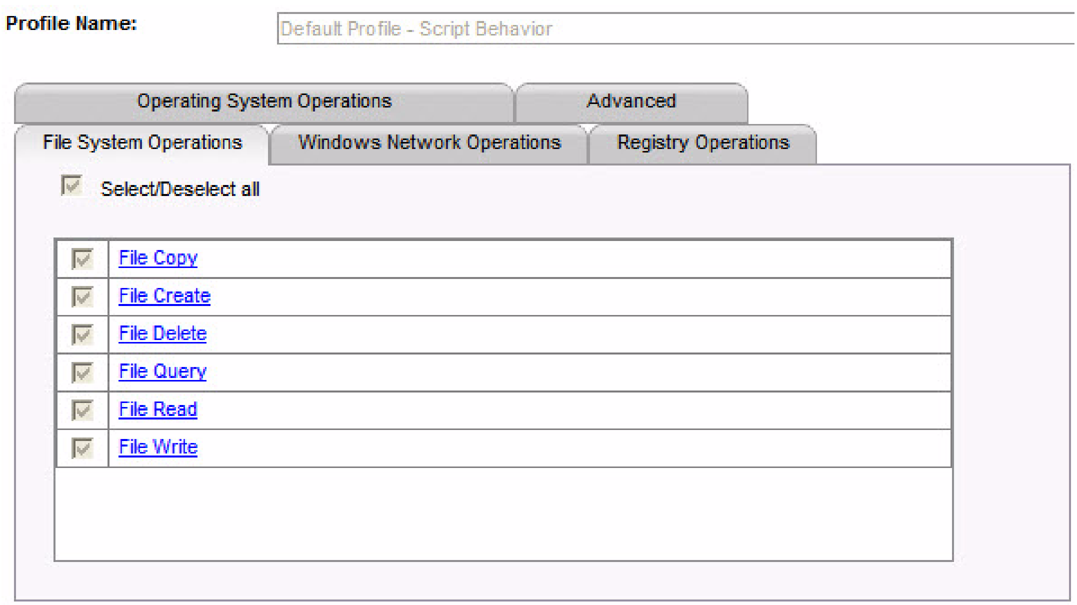
□	Default Profile - Script Behavior
☑	Higher Sensitivity Script Behavior Profile
□	Higher Sensitivity Vulnerability Anti.dote Profile
□	M86 Basic Anti.dote Profile
□	M86 Basic Behavior Profile
□	Spyware Profile
□	Unscannable Active Content
□	Vulnerability Anti.dote Profile

Figure 3-97: Block Malicious Scripts by Behavior

The following table displays the Rule definitions:

Block Malicious Scripts by Behavior	
Action	Block
End-User Message	Malicious Behavior Detected
Conditions	
Behavior Profile (Scripts)	Default Profile – Script Behavior

The **Block Malicious Scripts by Behavior** rule refers to the Behavior Profile which can be found via **Policies → Condition Settings → Script Behavior → Default Profile – Script Behavior**.



Profile Name: Default Profile - Script Behavior

☑ Select/Deselect all

☑	File Copy
☑	File Create
☑	File Delete
☑	File Query
☑	File Read
☑	File Write

Figure 3-98: Behavior Profile (Script)

The Behavior Profile consists of selected behavior groups of the SWG Behavior Profile engine. Those groups are divided into the following three tabs:

- Advanced
- VB Script
- Java Script

VB and Java script tabs contains behaviors which are used in the context of VB/Java script. The Advanced tab contains behaviors which are not limited to the VB/Java script scope.

In this section you will find some examples and descriptions of the Advanced/VB Script/Java Script entries.

Rule Demonstration:

Advanced Tab - Dangerous ActiveX Objects Remote Creation Protection, Remote File Read and Execution Protection

This entry will block content which tries to exploit ActiveX Objects in order to remotely read, write or execute files.

➲ **To test the Behavior Profile rule with selection of the Dangerous ActiveX Objects Remote Creation Protection, Remote File Read and Execution Protection profile:**

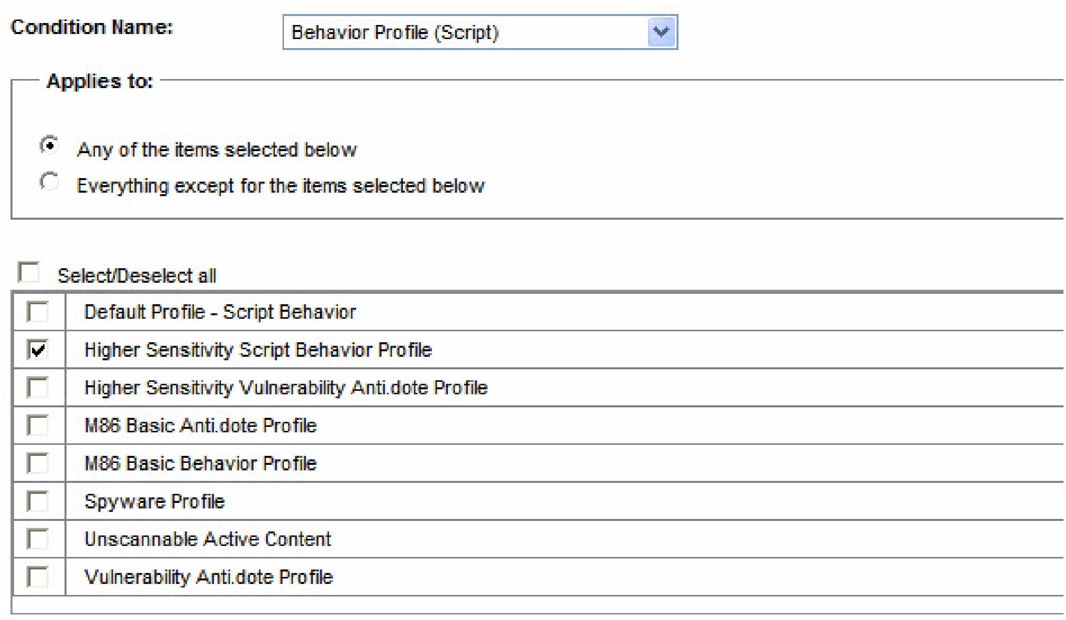
1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/runDir.htm

   This link will run the Dir dos command on an unprotected machine.

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



Condition Name: Behavior Profile (Script)

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

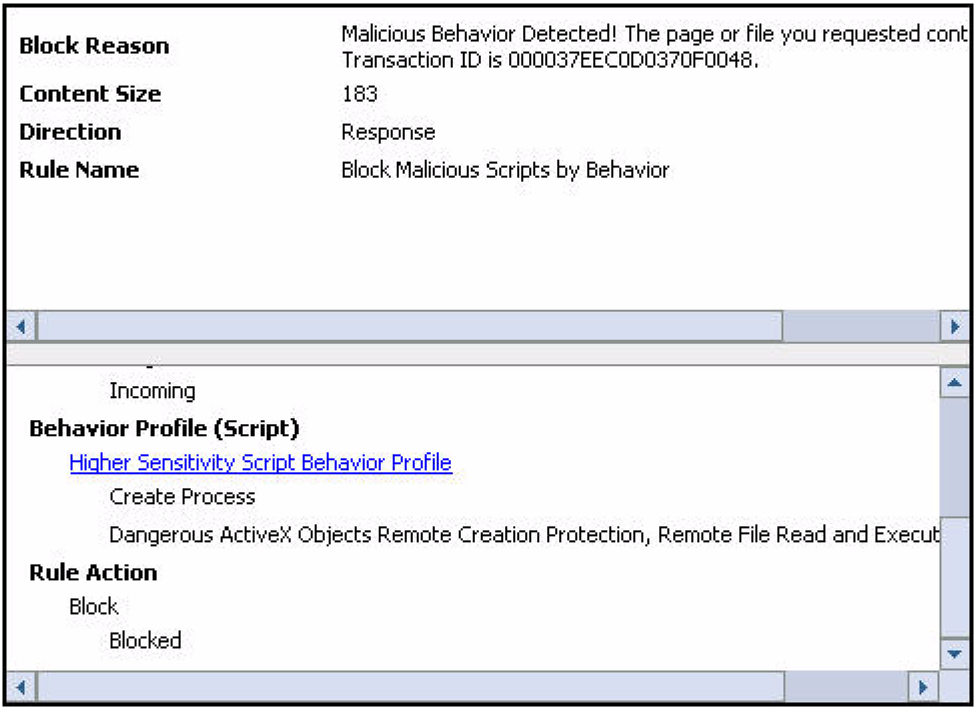
☐ Default Profile - Script Behavior
☑ Higher Sensitivity Script Behavior Profile
☐ Higher Sensitivity Vulnerability Anti.dote Profile
☐ M86 Basic Anti.dote Profile
☐ M86 Basic Behavior Profile
☐ Spyware Profile
☐ Unscannable Active Content
☐ Vulnerability Anti.dote Profile

Figure 3-99: Page Blocked -Malicious Behavior

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▸☰ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason Malicious Behavior Detected! The page or file you requested cont
Transaction ID is 000037EEC0D0370F0048.

Content Size 183

Direction Response

Rule Name Block Malicious Scripts by Behavior

Incoming

Behavior Profile (Script)

Higher Sensitivity Script Behavior Profile

Create Process

Dangerous ActiveX Objects Remote Creation Protection, Remote File Read and Execut

Rule Action

Block

Blocked

Figure 3-100: Response: Malicious Behavior

Advanced tab: Location. Generic Shellcode Execution

➲ **To test the Behavior Profile rule with selection of the Generic Shellcode execution:**

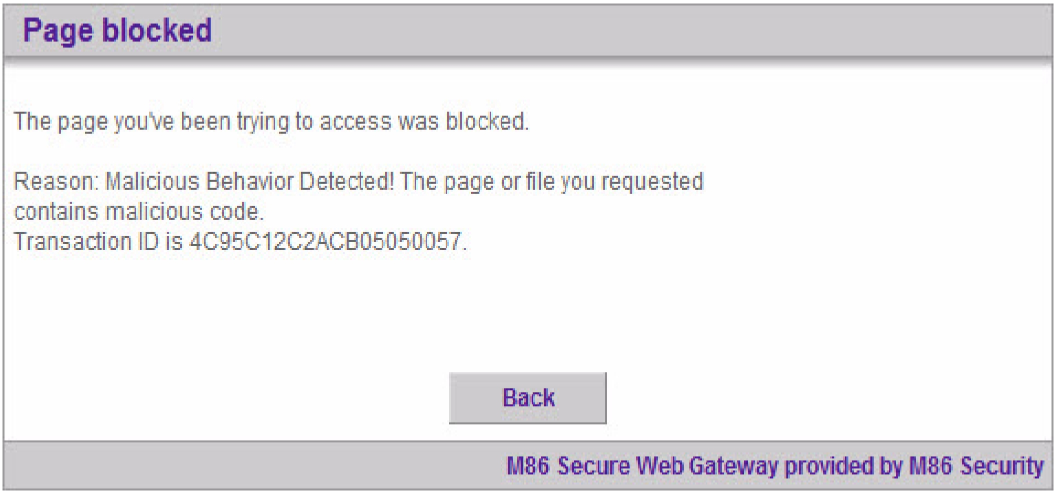
Code Execution Vulnerability:

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/Menus.js

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:


Page blocked

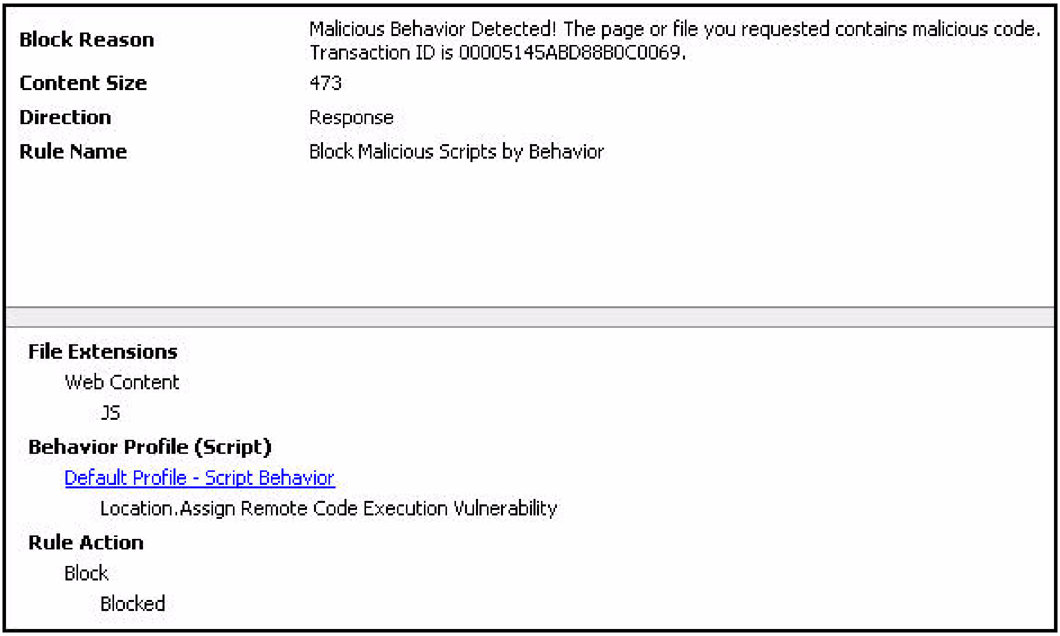
The page you've been trying to access was blocked.

Reason: Malicious Behavior Detected! The page or file you requested contains malicious code.
Transaction ID is 4C95C12C2ACB05050057.

Figure 3-101: Page Blocked: Malicious Behavior

NOTES: *If you have an Anti-Virus engine enabled - this file will be caught by Block Known Virus rule as it is placed higher up in the Security Policy. Navigate to the Logs as detailed below to see further details on other rules that block this file.*

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click ▸☰ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason Malicious Behavior Detected! The page or file you requested contains malicious code. Transaction ID is 00005145ABD88B0C0069.

Content Size 473

Direction Response

Rule Name Block Malicious Scripts by Behavior

File Extensions
Web Content
JS

Behavior Profile (Script)
Default Profile - Script Behavior
Location.Assign Remote Code Execution Vulnerability

Rule Action
Block
Blocked

Figure 3-102: Response: Malicious Behavior

JavaScript tab: Operating System Operations

➲ **To test the Behavior Profile rule with selection of the Operating System Operations options:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/Demo2.htm

   This link will attempt to add scripts to your desktop:

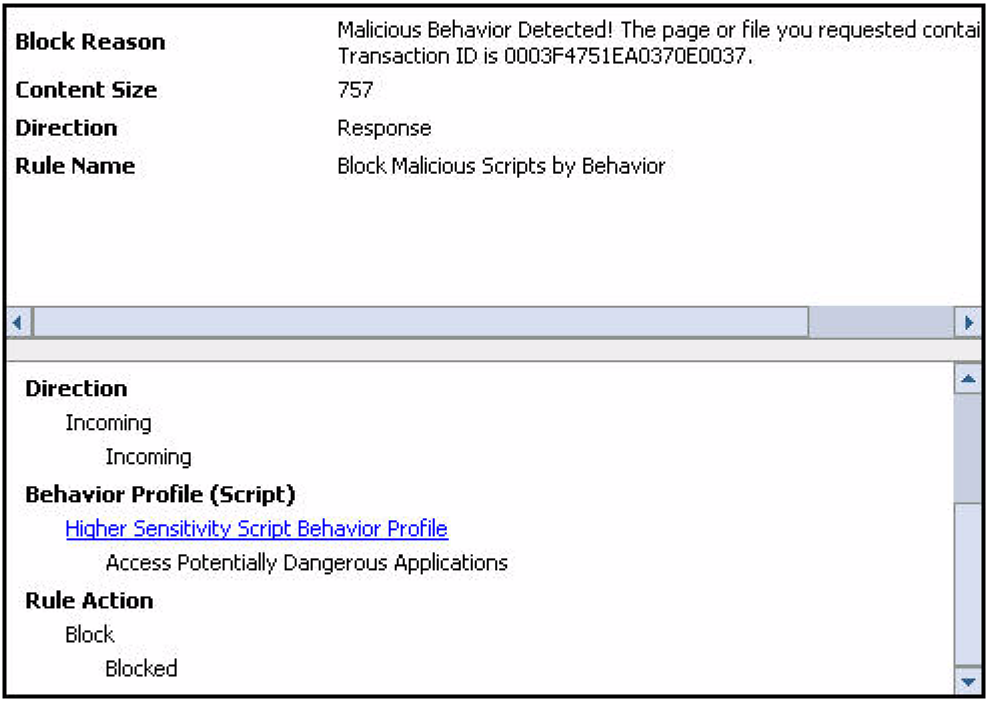
2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▸☰ and select Details. The Transaction Detail tabs include Transaction,

User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	Malicious Behavior Detected! The page or file you requested contai Transaction ID is 0003F4751EA0370E0037.
Content Size	757
Direction	Response
Rule Name	Block Malicious Scripts by Behavior

Direction
- Incoming
  - Incoming

Behavior Profile (Script)
- Higher Sensitivity Script Behavior Profile
  - Access Potentially Dangerous Applications

Rule Action
- Block
  - Blocked

Figure 3-103: Response: Malicious Behavior

This page was blocked due to **Access Potentially Dangerous Applications** violation.

JavaScript tab: File System Operations

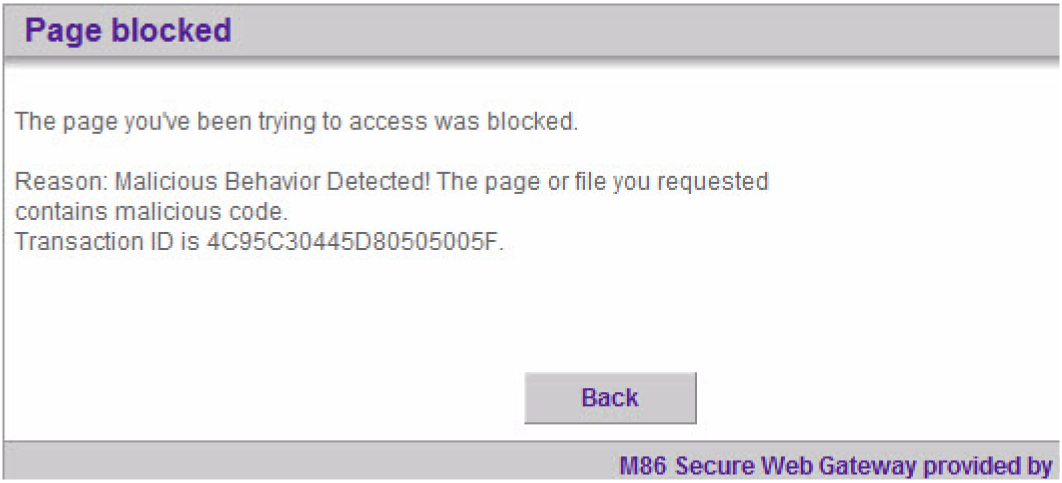
➲ **To test the Behavior Profile rule with selection of the File System Operations options:**

1. Copy and paste the following URL into your browser:

http://www.m86security.com/EVG/Active_Object.js

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



Page blocked

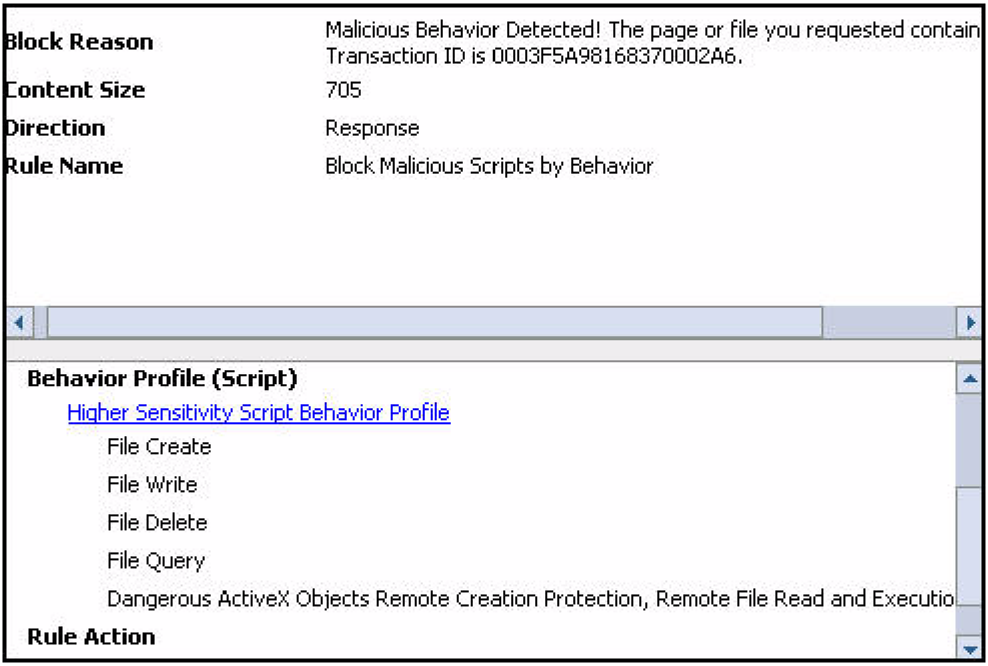
The page you've been trying to access was blocked.

Reason: Malicious Behavior Detected! The page or file you requested contains malicious code.
Transaction ID is 4C95C30445D80505005F.

M86 Secure Web Gateway provided by

Figure 3-104: Page Blocked: Malicious Behavior

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	Malicious Behavior Detected! The page or file you requested contain Transaction ID is 0003F5A98168370002A6.
Content Size	705
Direction	Response
Rule Name	Block Malicious Scripts by Behavior

Behavior Profile (Script)

Higher Sensitivity Script Behavior Profile

File Create

File Write

File Delete

File Query

Dangerous ActiveX Objects Remote Creation Protection, Remote File Read and Executio

Rule Action

Figure 3-105: Response: Malicious Behavior

This page was blocked due to multiple security policy violations such as File Query, File Write, File Copy, File Create, File Delete (entries of the File System Operations group).

VBScript tab: Windows network operation

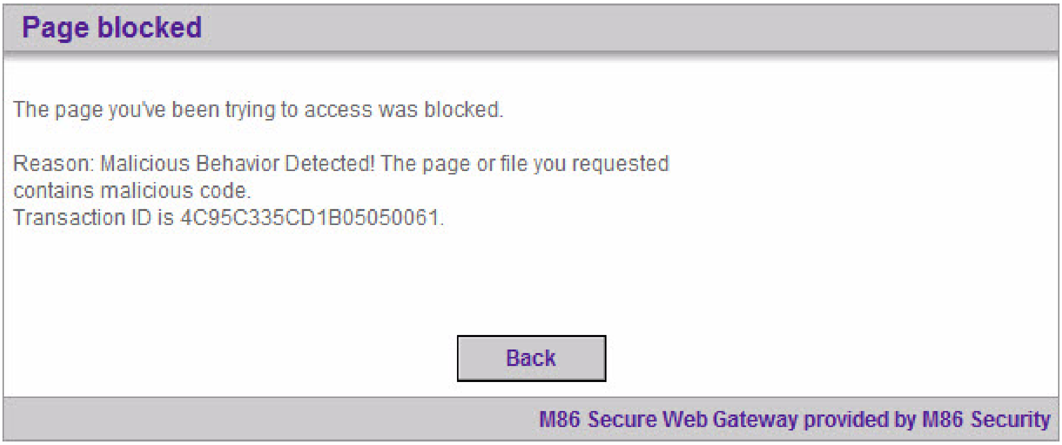
➲ **To test the Behavior Profile rule with selection of the Windows Network Operation option:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/WriteFileDemo.vbs

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:

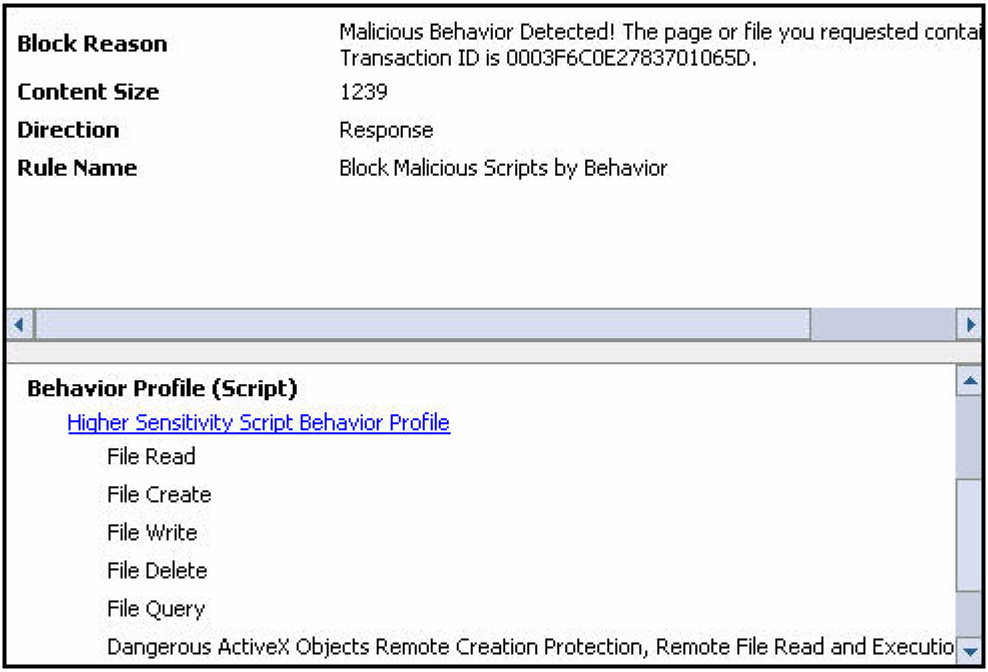


The page you've been trying to access was blocked.

Reason: Malicious Behavior Detected! The page or file you requested contains malicious code.
Transaction ID is 4C95C335CD1B05050061.

Figure 3-106: Page Blocked - Malicious Behavior

3. Return to the Management Console and select the **Logs** → **View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click ▶☰ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	Malicious Behavior Detected! The page or file you requested contai Transaction ID is 0003F6C0E2783701065D.
Content Size	1239
Direction	Response
Rule Name	Block Malicious Scripts by Behavior

Behavior Profile (Script)

Higher Sensitivity Script Behavior Profile

File Read

File Create

File Write

File Delete

File Query

Dangerous ActiveX Objects Remote Creation Protection, Remote File Read and Executio

Figure 3-107: Response: Malicious Behavior

VBScript tab: Registry Operations

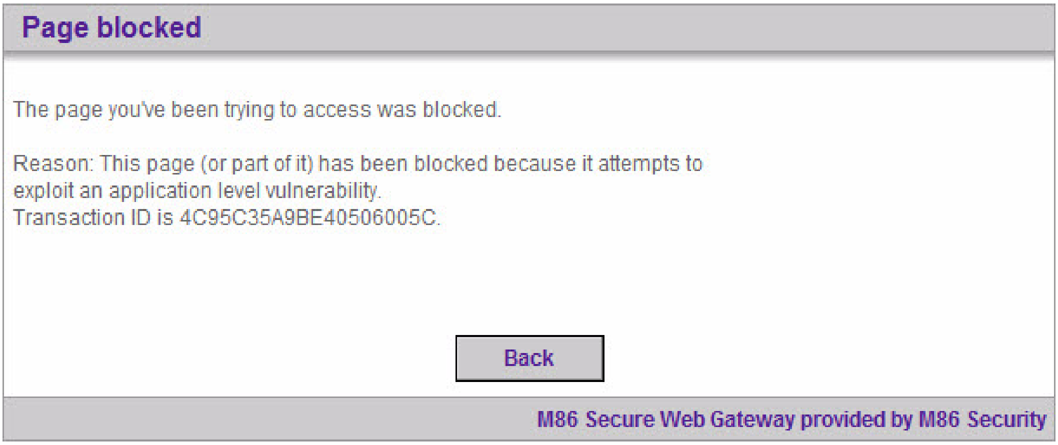
➲ **To test the Behavior Blocking Profile rule with selection of the Registry Operations:**

1. Copy and paste the following URL into your browser.

   www.finjan.com/evg/upload.vbs

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



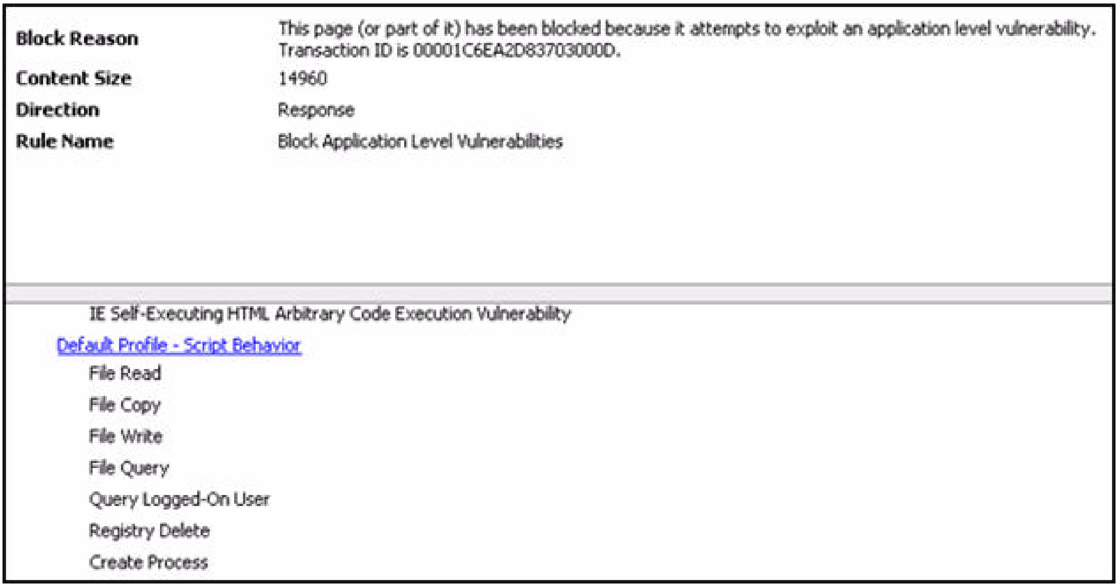
Page blocked

The page you've been trying to access was blocked.

Reason: This page (or part of it) has been blocked because it attempts to exploit an application level vulnerability.
Transaction ID is 4C95C35A9BE40506005C.

Figure 3-108: Page Blocked - Browser/OS Vulnerability

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.
4. In the same row as the blocked transaction, click ▸☰ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.
5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	This page (or part of it) has been blocked because it attempts to exploit an application level vulnerability. Transaction ID is 00001C6EA2D83703000D.
Content Size	14960
Direction	Response
Rule Name	Block Application Level Vulnerabilities

IE Self-Executing HTML Arbitrary Code Execution Vulnerability

Default Profile - Script Behavior

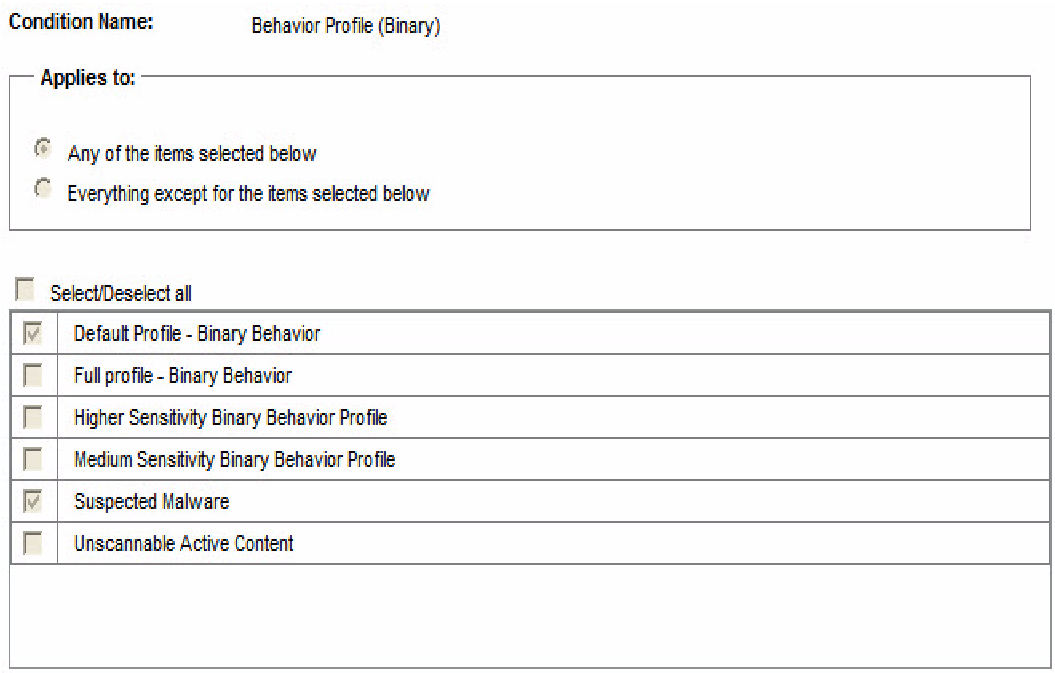
- File Read
- File Copy
- File Write
- File Query
- Query Logged-On User
- Registry Delete
- Create Process

Figure 3-109: Response: Browser/OS Vulnerability

This page was blocked due to multiple security policy violations, including Registry restricted operation – **Registry Delete**.

Block Malicious ActiveX, Java Applets and Executables

The **Block Malicious ActiveX, Java Applets and Executables** rule uses the M86 Propietary Behavior Profile (Binary) engine. This is a unique security engine, designed to identify and block malicious content by identifying combinations of operations, parameters, script manipulations and other exploitation techniques for a given piece of content.



Condition Name: Behavior Profile (Binary)

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

☑	Default Profile - Binary Behavior
□	Full profile - Binary Behavior
□	Higher Sensitivity Binary Behavior Profile
□	Medium Sensitivity Binary Behavior Profile
☑	Suspected Malware
□	Unscannable Active Content

Figure 3-110: Block Malicious ActiveX, Java Applets and Executables rule

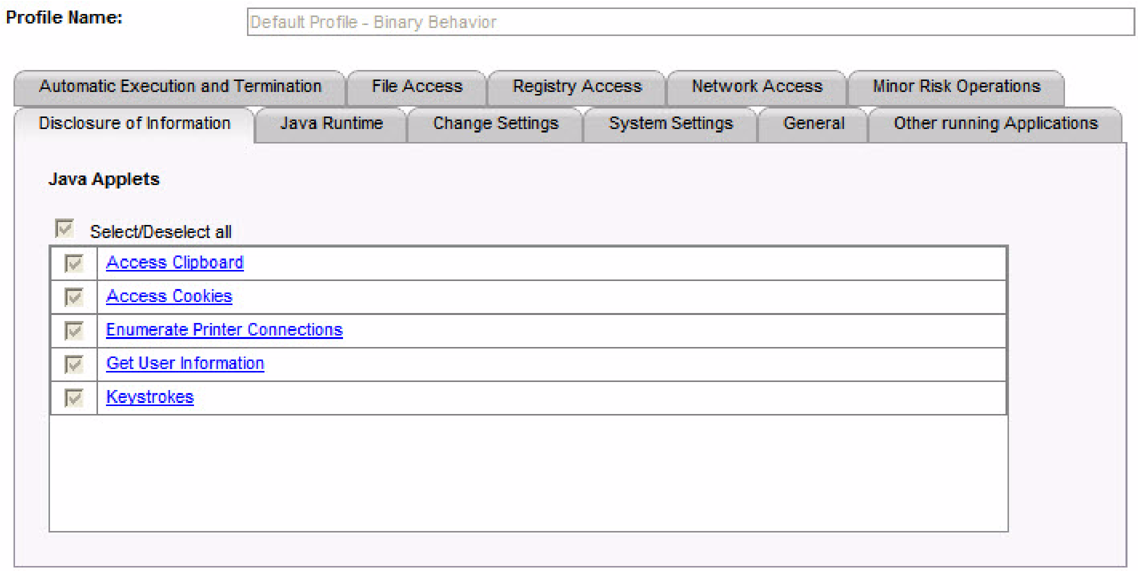
The following table displays the definitions:

Block Malicious ActiveX, Java Applets and Executables	
Action	Block
End-User Message	Malicious Behavior Detected
Conditions	
Behavior Profile	Default Profile - Binary Behavior (Strict) Suspected Malware (Strict) Medium Sensitivity Binary Behavior Profile (Medium)

Further Information:

- If Default Profile - Binary Behavior is selected then this rule prevents end-users from downloading most executables such as setup.exe files and is therefore only included in the Strict Security Policy. **This is the only difference between the Medium and Strict Security Policies.**

- The **Binary Behavior** information can be found via **Policies → Condition Settings → Binary Behavior → Default Profile – Binary Behavior**.



Profile Name: Default Profile - Binary Behavior

Java Applets

☑ Select/Deselect all

☑ Access Clipboard
☑ Access Cookies
☑ Enumerate Printer Connections
☑ Get User Information
☑ Keystrokes

Figure 3-111: Behavior Profile (Binary)

The **Behavior Profile** consists of selected behavior groups of the **Behavior Profile engine**. Those groups are divided into 2 areas:

- ActiveX and Executables
- Java Applets

Rule Demonstration:

Java Applets

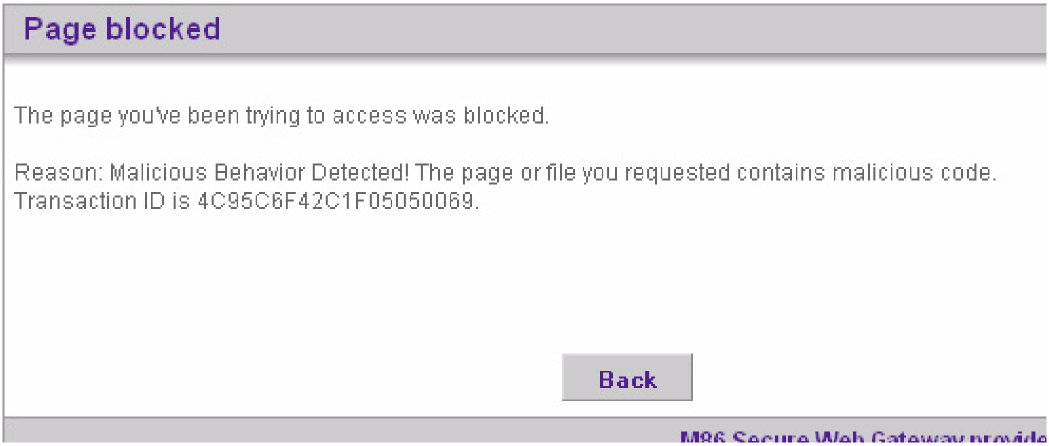
➲ **To test the Block Malicious ActiveX, Java Applets and Executables rule with selection of the Behavior Blocking: Java Applets**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/readFile.class

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

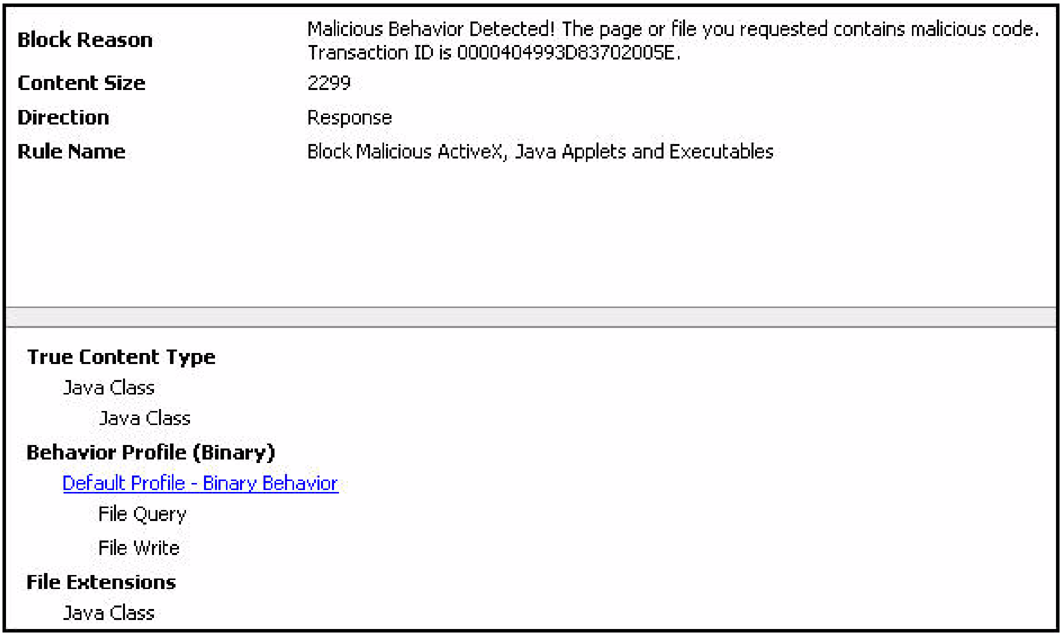
Reason: Malicious Behavior Detected! The page or file you requested contains malicious code.
Transaction ID is 4C95C6F42C1F05050069.

Figure 3-112: Error Messages: Malicious Behavior

3. Return to the Management Console and select the **Logs** → **View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Block Reason	Malicious Behavior Detected! The page or file you requested contains malicious code. Transaction ID is 0000404993D83702005E.
Content Size	2299
Direction	Response
Rule Name	Block Malicious ActiveX, Java Applets and Executables

True Content Type
- Java Class
  - Java Class

Behavior Profile (Binary)
- Default Profile - Binary Behavior
  - File Query
  - File Write

File Extensions
- Java Class

Figure 3-113: Response: Malicious Behavior

ActiveX and Executables Violation:

➲ **To test the Block Malicious ActiveX, Java Applets and Executables rule with selection of the Behavior Blocking: ActiveX and Executables Violation:**

1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/FinjanEmptyDemo.zip

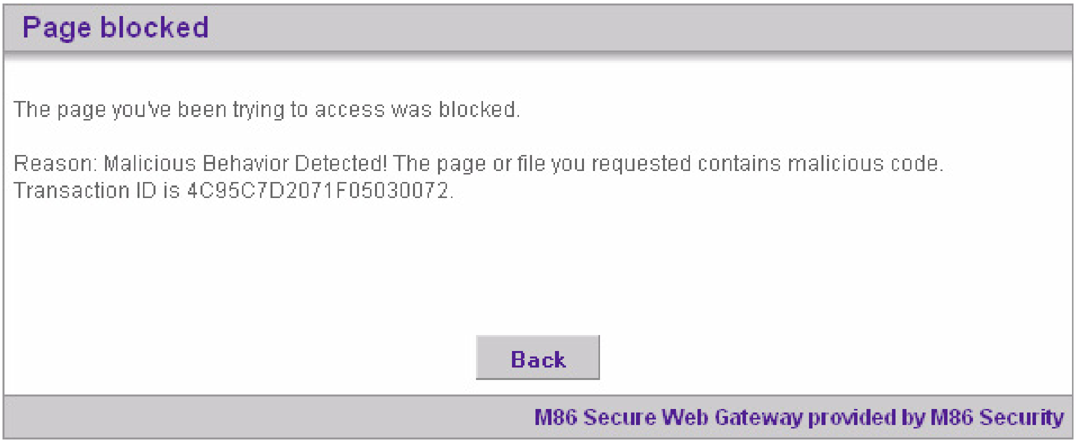
This URL contains an exe file which violates the following restricted behaviors:

- File Read
- File Write

- Terminate Process
- Potentially Dangerous Process: Debugging Functions
- Potentially Dangerous Memory Management Functions
- Dynamic Link Library Invocation Functions

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

The following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

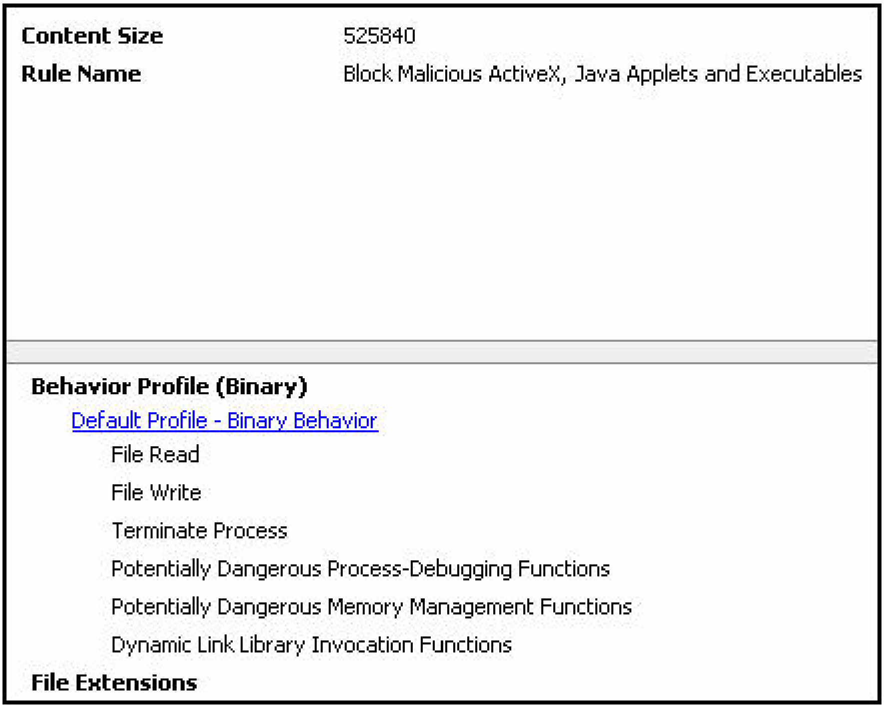
Reason: Malicious Behavior Detected! The page or file you requested contains malicious code.
Transaction ID is 4C95C7D2071F05030072.

Figure 3-114: Page Blocked - Malicious Behavior

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction, User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



Content Size	525840
Rule Name	Block Malicious ActiveX, Java Applets and Executables

Behavior Profile (Binary)

Default Profile - Binary Behavior

File Read

File Write

Terminate Process

Potentially Dangerous Process-Debugging Functions

Potentially Dangerous Memory Management Functions

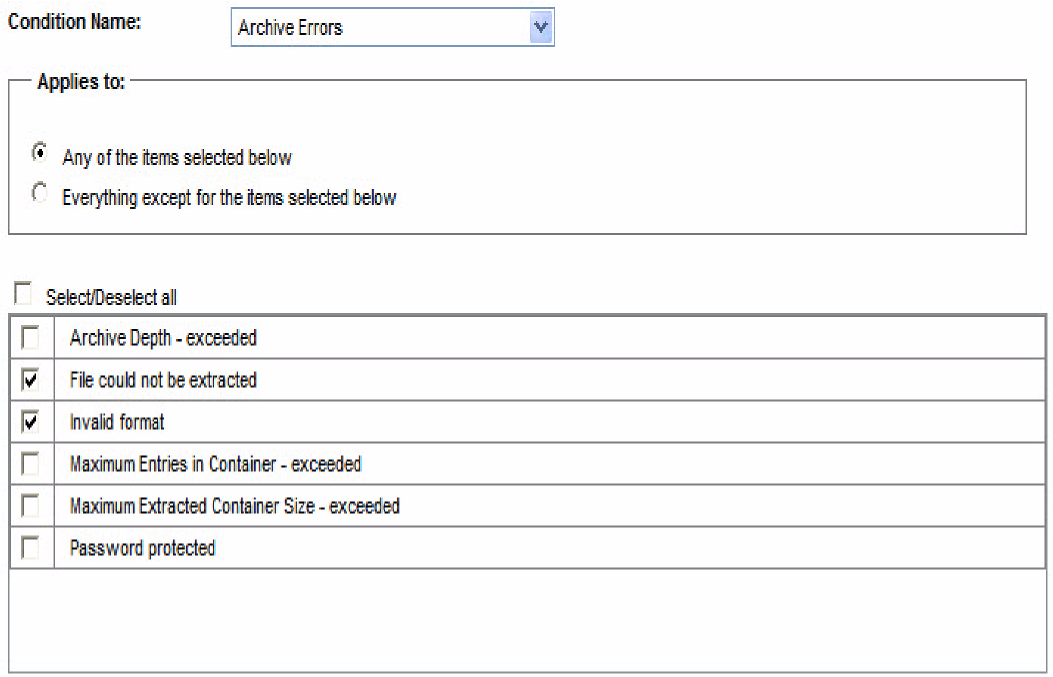
Dynamic Link Library Invocation Functions

File Extensions

Figure 3-115: Response: Malicious Behavior

Block Illegitimate Archives (Including Password-Protected Archives)

The **Block Illegitimate Archives (Including Password Protected Archives)** rule blocks attacks that try to use malformed archives. It also blocks password protected archives since they cannot be scanned.



Condition Name: Archive Errors

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all

□	Archive Depth - exceeded
☑	File could not be extracted
☑	Invalid format
□	Maximum Entries in Container - exceeded
□	Maximum Extracted Container Size - exceeded
□	Password protected

Figure 3-116: Block Illegitimate Archives (Including Password Protected Archives)

The following table displays the Rule Editor definitions:

Block Illegitimate Archives (Including Password Protected Archives)	
Action	Block
End-User Message	Container Violation
Conditions	
Archive Errors	File could not be extracted, Invalid format, Password protected

Rule Demonstration:

➲ **To test the Block Illegitimate Archives (Including Password Protected Archives) rule:**

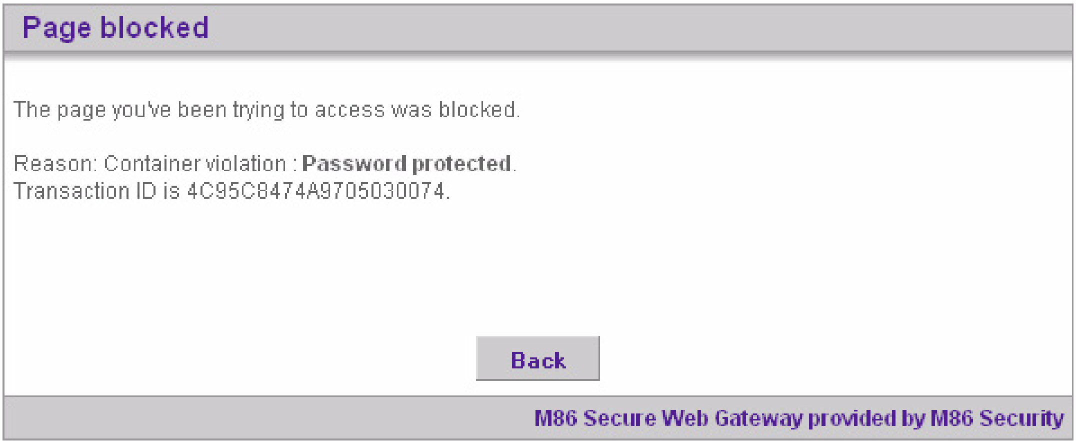
1. Copy and paste the following URL into your browser:

   http://www.m86security.com/EVG/demo.zip

   This link will try to exploit ZIP file vulnerability which causes a denial of service.

2. To connect to the site, type in the username: **getevg** and password: **HurNoc45**, and click **OK**.

A download status page appears. After this page, the following error message is displayed:



Page blocked

The page you've been trying to access was blocked.

Reason: Container violation : **Password protected**.
Transaction ID is 4C95C8474A9705030074.

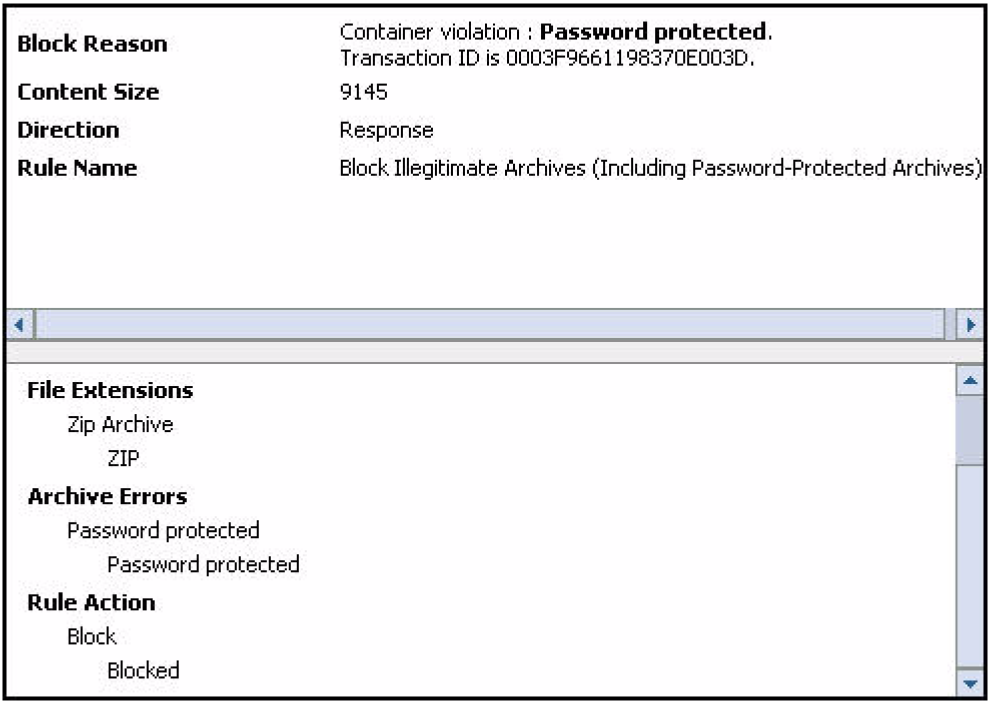
Figure 3-117: Page Blocked - Illegitimate Archives

3. Return to the Management Console and select the **Logs → View Web Logs** menu in the Main Navigation bar.

4. In the same row as the blocked transaction, click ▤ and select Details. The Transaction Detail tabs include Transaction,

User, Policy Enforcement, Content and Scanning Server details.

5. In the Transaction Details tree, click **Request/Response** to obtain further information on the Request and Response phases of this transaction.



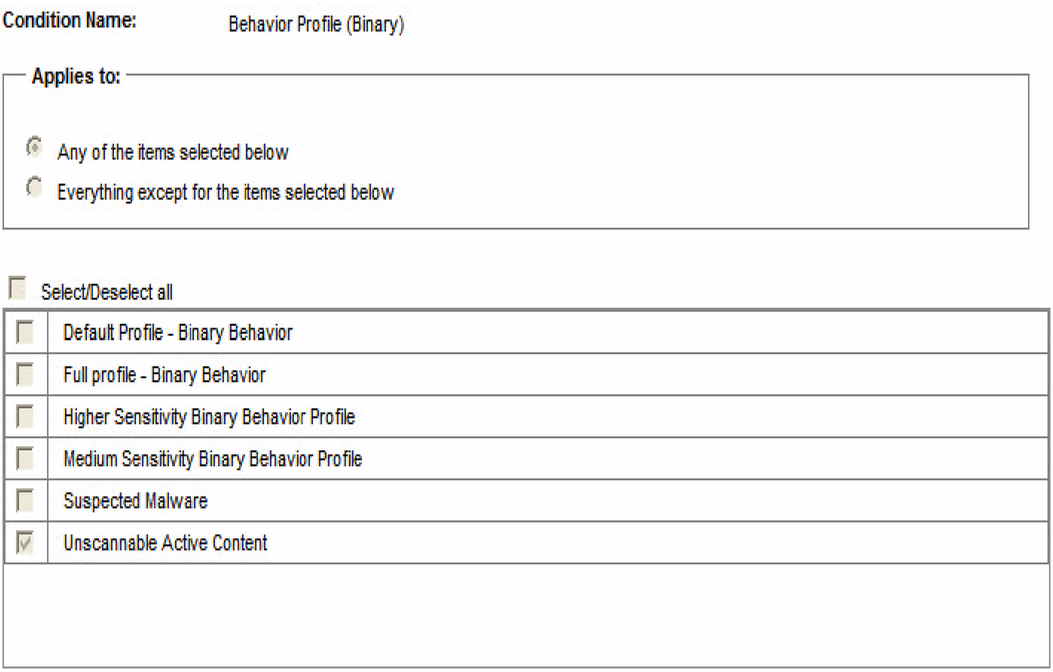
Block Reason	Container violation : **Password protected.** Transaction ID is 0003F9661198370E003D.
Content Size	9145
Direction	Response
Rule Name	Block Illegitimate Archives (Including Password-Protected Archives)

File Extensions
Zip Archive
ZIP
Archive Errors
Password protected
Password protected
Rule Action
Block
Blocked

Figure 3-118: Response: Illegitimate Archives

Block Unscannable ActiveX, Java Applets and Executables

The **Block Unscannable ActiveX, Java Applets and Executables** rule blocks unscannable active content.



Condition Name: Behavior Profile (Binary)

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□	Default Profile - Binary Behavior
□	Full profile - Binary Behavior
□	Higher Sensitivity Binary Behavior Profile
□	Medium Sensitivity Binary Behavior Profile
□	Suspected Malware
☑	Unscannable Active Content

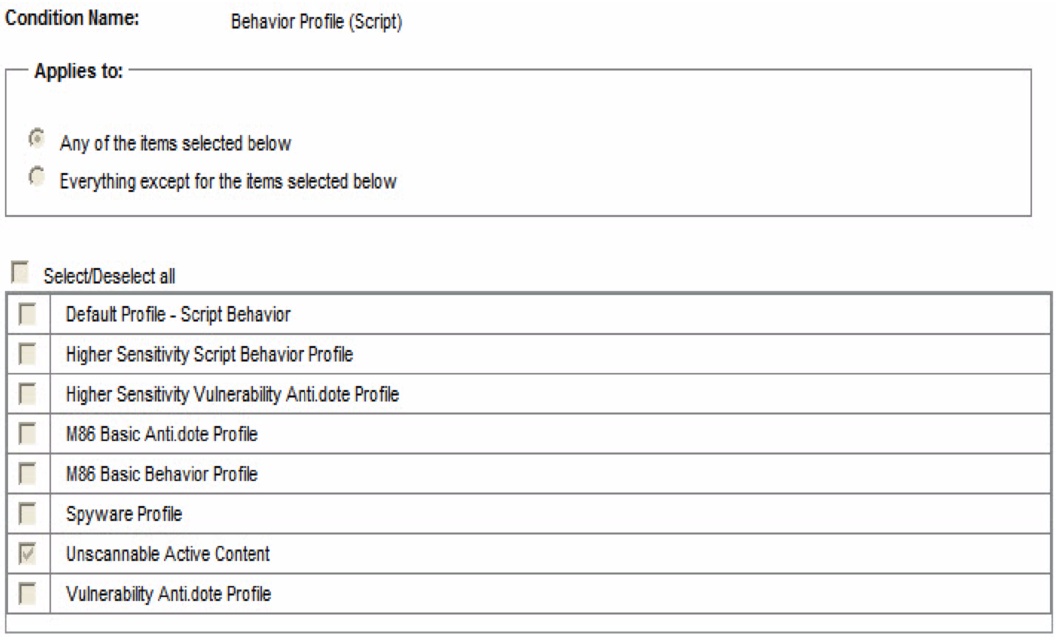
Figure 3-119: Block Unscannable ActiveX, Java Applets and Executables

The following table displays the definitions:

Block Unscannable ActiveX, Java Applets and Executables	
Action	Block
End-User Message	Unscannable Content Detected
Conditions	
True Content Type	Active Binary Content
Behavior Profile (Binary)	Unscannable Active Content

Block Unscannable Web Pages and Scripts

The **Block Unscannable Web Pages and Scripts** rule blocks unscannable active content since formatting content in such a way is considered suspicious behavior, and malicious behavior cannot be detected in such pages.



Condition Name: Behavior Profile (Script)

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

□ Select/Deselect all

□	Default Profile - Script Behavior
□	Higher Sensitivity Script Behavior Profile
□	Higher Sensitivity Vulnerability Anti.dote Profile
□	M86 Basic Anti.dote Profile
□	M86 Basic Behavior Profile
□	Spyware Profile
☑	Unscannable Active Content
□	Vulnerability Anti.dote Profile

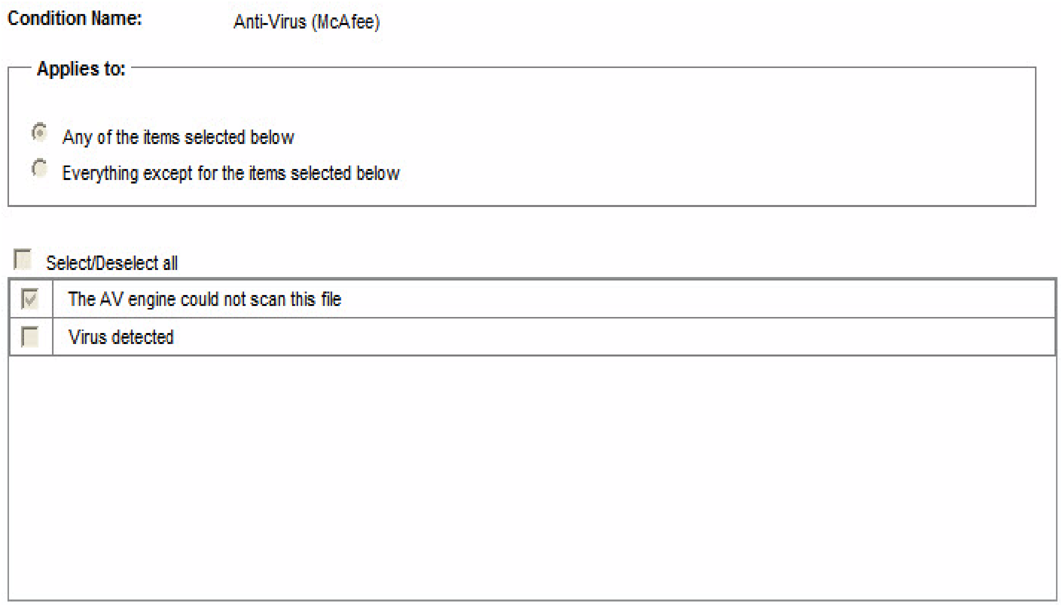
Figure 3-120: Block Unscannable Web Pages and Scripts

The following table displays the Rule Editor definitions:

Block Unscannable Web Pages and Scripts	
Action	Block
End-User Message	Malicious Behavior Detected
Conditions	
True Content Type	Java Script, MS Encoded Java Script, Text File, VB Script, Web Page
Behavior Profile (Binary)	Unscannable Active Content

Block Unscannable (McAfee / Sophos / Kaspersky)

The **Block Unscannable (McAfee/Sophos/Kaspersky)** rule blocks unscannable content. Content which is not scannable by the traditional Anti-Virus engine is always blocked since there is no risk estimation for it, and since formatting content in such way is, in and of itself, very suspicious behavior. You need a license for one of these Anti-Virus engines.



Condition Name: Anti-Virus (McAfee)

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

☐ Select/Deselect all

☑	The AV engine could not scan this file
☐	Virus detected

Figure 3-121: Block Unscannable (McAfee)

The following table displays the definitions:

Block Unscannable (McAfee/Sophos/Kaspersky)	
Action	Block
End-User Message	Blocked since AV could not scan

Block Unscannable (McAfee/Sophos/Kaspersky)	
Conditions	
Anti-Virus (McAfee/ Sophos/ Kaspersky)	The Anti-Virus engine could not scan this file

M86 HTTPS Policy

Overview of HTTPS Policy

The M86 HTTPS Policy defines security in terms of checking certificates associated with certain websites, decrypting information and acting on the content.

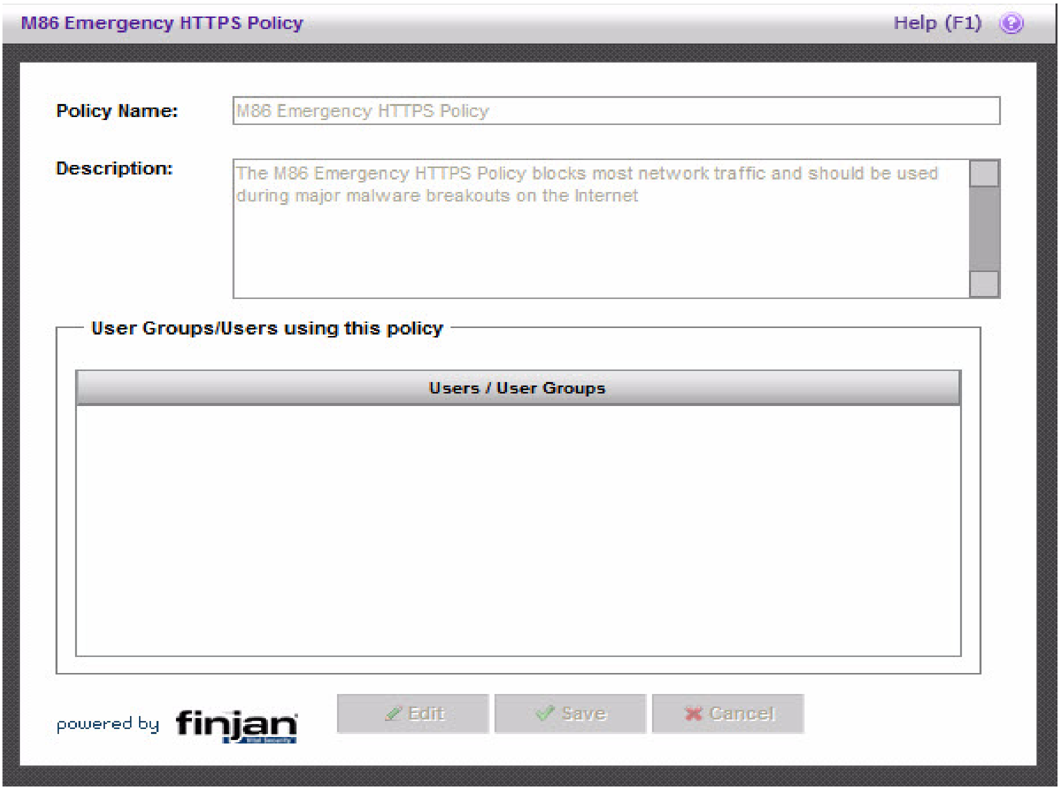
Policy Architecture

The **M86 HTTPS Policy** is comprised of a rule that describes how to handle encrypted Web content passing through the system. **Rules** in the HTTPS Policy are built from a combination of **Conditions** which can also be configured. **Conditions** incorporate values chosen from URL lists, URL Categorization groups, and Certificate Validations.

HTTPS Policy Details

Clicking on the **M86 HTTPS Policy** for example, on the left-hand side of the pane displays the following information:

- Policy Name
- Description
- Assigned Users/User Groups



M86 Emergency HTTPS Policy

Policy Name: M86 Emergency HTTPS Policy

Description: The M86 Emergency HTTPS Policy blocks most network traffic and should be used during major malware breakouts on the Internet

User Groups/Users using this policy

Users / User Groups

Figure 4-1: M86 HTTPS Policy Details

M86 HTTPS Policy Rule Details

The Rule Details screen defines the **Action** and **End User Message** for the corresponding rule.

- **Action:** Each rule has a corresponding **Action**:
  - **Bypass:** Certificate validation will not be performed by the system. No security inspection will take place.
  - **Inspect Content (default):** HTTPS rules and Security rules scanning is carried out.
  - **User approval:** Sends an approval page to the end-user for each new HTTPS site that is accessed. This is sent for situations

where the certificate is valid but user approval is required to decrypt traffic for this site or where there were certificate mismatches and the end-user is given the choice to continue or not. If the end-user chooses not to approve the transaction, the connection is closed. This is similar to the Coach action for Security Rules.

- **Block HTTPS:** Sites that have certificate errors are blocked.

- **End-User Message:** Each rule that has the **Inspect Content** or **User Approval** or **Block HTTPS** action can have a reason which is selected from a drop-down list. This reason is displayed in a message to the end-user which can be configured via **End-User Messages → Block/Warn Messages.** This reason can be selected from a list of pre-defined reasons or created by the administrator.

  Alternatively, you can select **Do not display End-User Message** if you do not want to display a message to the end-user.

Conditions

Each rule may include several conditions; all of which must be met in order for the rule to be followed. The following Conditions are available:

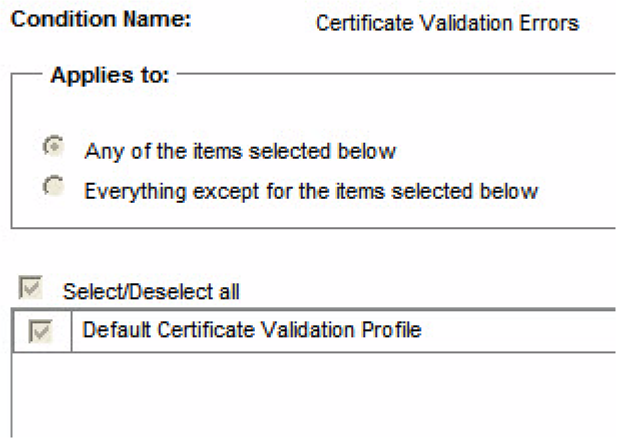
- **Certificate Validation:** This condition includes many different types of certificate validation errors. These are provided with a Default HTTPS profile under the Security Engines tab.
- **URL Filtering (Websense/IBM):** This condition can be used to apply rules based on the type or category of the requested site.
- **URL Lists**: This condition refers to lists of URLs – both predefined and configurable.

M86 HTTPS Policy Rules

The following Rule is included in the M86 HTTPS Policy.

Block Certificate Validation Errors

The only rule in the M86 HTTPS Policy is the **Block Certificate Validation Errors**. This rule blocks sites containing invalid or missing digital certificates.



Condition Name: Certificate Validation Errors

Applies to:

● Any of the items selected below

○ Everything except for the items selected below

☑ Select/Deselect all

☑ Default Certificate Validation Profile

Figure 4-2: Block Certificate Validation Errors

The following table displays the Rule definitions:

Block Certificate Validation Errors	
Action	Block HTTPS
End-User Message	Certificate Validation Mismatch
Conditions	
Certificate Validation Errors	Default Certificate Validation Profile

IMPORTANT: It is important in any customer-defined HTTPS Policy to always have the first rule allowing content

Emergency Policies

Overview

The M86 Emergency Policy and M86 HTTPS Emergency Policy were designed for cases where, for example, the Internet has encountered a massive infectious attack and/or for cases where the organization has been infected by malicious code.

The Emergency Policies prevent/minimize damage by blocking most of the network traffic while still enabling access to some predefined important web sites (e.g. Windows Update).

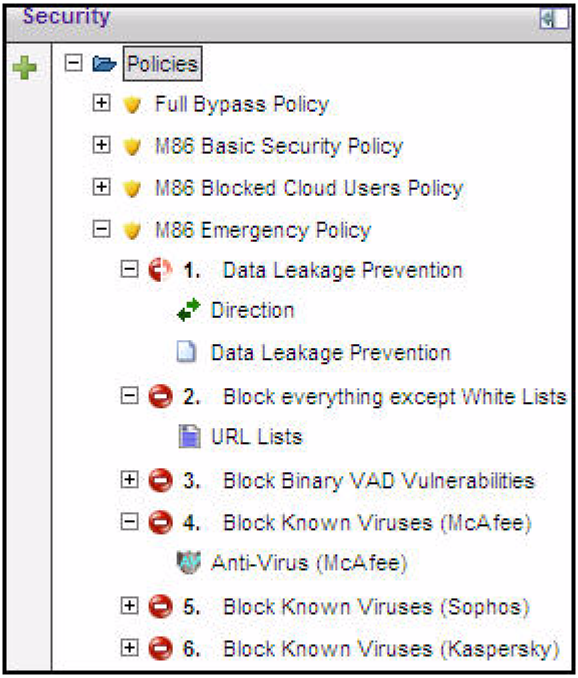

Security
Policies
Full Bypass Policy
M86 Basic Security Policy
M86 Blocked Cloud Users Policy
M86 Emergency Policy
1. Data Leakage Prevention
Direction
Data Leakage Prevention
2. Block everything except White Lists
URL Lists
3. Block Binary VAD Vulnerabilities
4. Block Known Viruses (McAfee)
Anti-Virus (McAfee)
5. Block Known Viruses (Sophos)
6. Block Known Viruses (Kaspersky)

Figure 5-1: M86 Emergency Policy

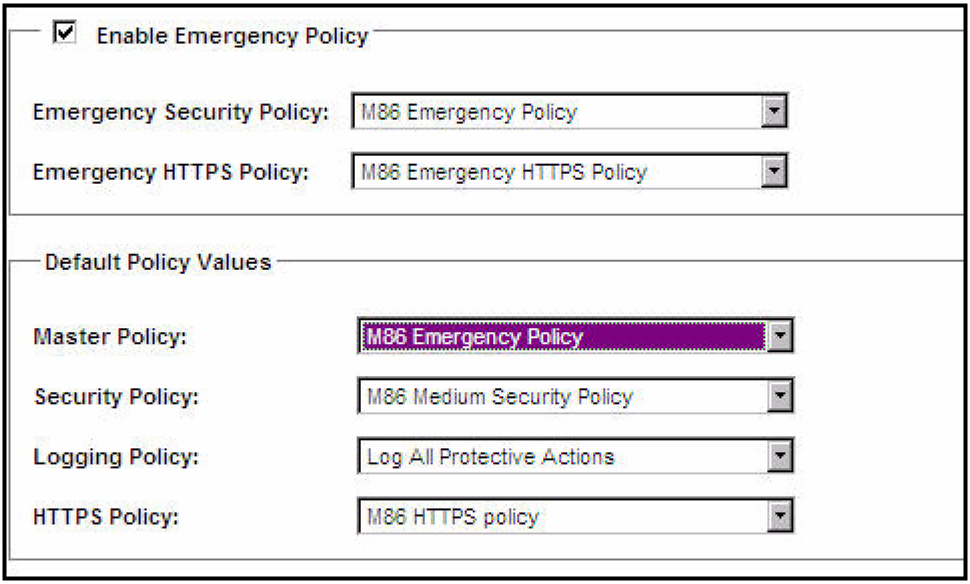
Assigning Emergency Policies

One way of assigning the M86 Emergency Policy and M86 HTTPS Emergency Policy is to enforce these Policies on all traffic passing through the system.

➲ **To enforce the Emergency Policy system-wide:**

1. Navigate to **Policies → Default Policy Settings**.
2. In the **Default Policy Settings** screen, click **Edit**.
3. Click **Enable Emergency Policy** and choose the required Security/HTTPS Emergency Policies from the drop-down list.
4. Click **Save** at the bottom of the page, and then click .

Another option is to assign specific Users or User Groups to the M86 Emergency Policies.



☑ Enable Emergency Policy

Emergency Security Policy: M86 Emergency Policy

Emergency HTTPS Policy: M86 Emergency HTTPS Policy

Default Policy Values

Master Policy: M86 Emergency Policy

Security Policy: M86 Medium Security Policy

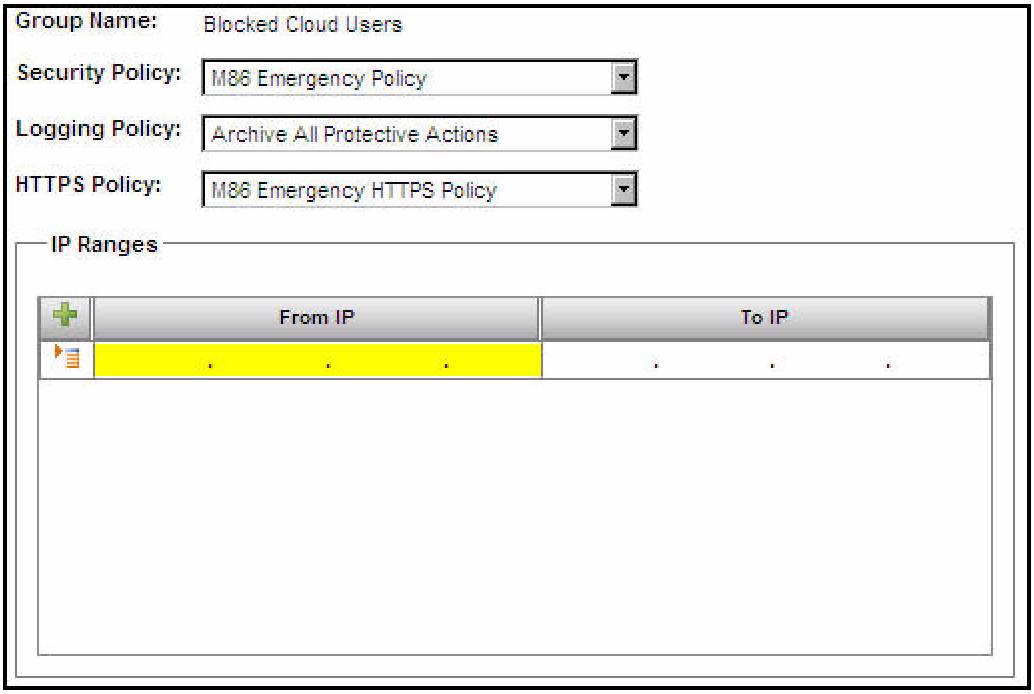
Logging Policy: Log All Protective Actions

HTTPS Policy: M86 HTTPS policy

Figure 5-2: Setting Emergency Policy System-wide

➲ To assign users to the Emergency Policy:

1. Navigate to the Users tab in the Main Navigation console and select the required User Group (or User).
2. Click **Edit** to change the details.
3. In the Security Policies drop-down list, select the **M86 Emergency Policy**. In the HTTPS Policies drop-down list, select the M86 HTTPS Emergency Policy



Group Name: Blocked Cloud Users

Security Policy: M86 Emergency Policy

Logging Policy: Archive All Protective Actions

HTTPS Policy: M86 Emergency HTTPS Policy

IP Ranges

	From IP	To IP
	. . .	. . .

Figure 5-3: Assigning Emergency Policy User Specific

4. Click **Save** and then click ⇊ to commit changes.

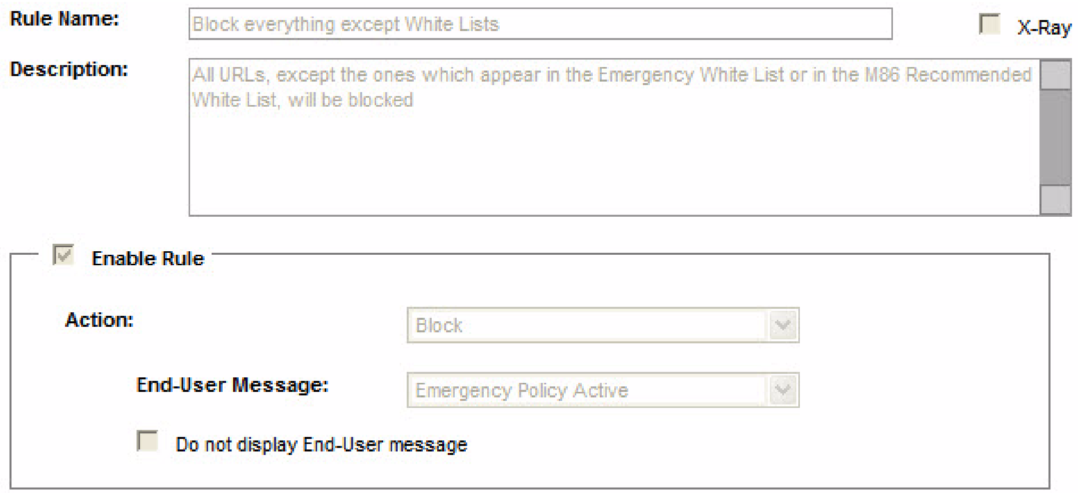
M86 Emergency Policy Rules

The M86 Emergency Policy consists of three rules:

- Block Everything except White Lists
- Block Binary VAD Vulnerabilities
- Block Known Viruses (McAfee / Sophos / Kaspersky)

Block Everything except White Lists

The first rule listed in the M86 Emergency Policy is the **Block Everything except White Lists** rule. All URLs, except the ones which appear on the Emergency White List or on the M86 Recommended White List, will be blocked.



Rule Name: Block everything except White Lists

□ X-Ray

Description: All URLs, except the ones which appear in the Emergency White List or in the M86 Recommended White List, will be blocked

☑ Enable Rule

Action: Block

End-User Message: Emergency Policy Active

□ Do not display End-User message

Figure 5-4: Block everything except White Lists (Default Emergency Policy)

The following table displays the Rule definitions:

Block Everything except White Lists	
Action	Block
End-User Message	Emergency Policy Active
Conditions	
URL Lists	Everything **except** for: Emergency White List and M86 Recommended White List

Further information:

- The Emergency White List is a user-defined list of allowed sites. It is accessible via **Condition Settings → URL Lists → Emergency White List**. In this screen you can add/delete entries by selecting **Add/ Delete** in the right pane.
- The M86 Recommended White List can be viewed but not manipulated by the administrator.

Block Binary VAD Vulnerabilities

For information on this rule, please refer to Block Binary VAD Vulnerabilities.

Block Known Viruses (McAfee/Sophos/Kaspersky)

For information on this rule, please refer to Block Known Viruses (McAfee / Sophos / Kaspersky).

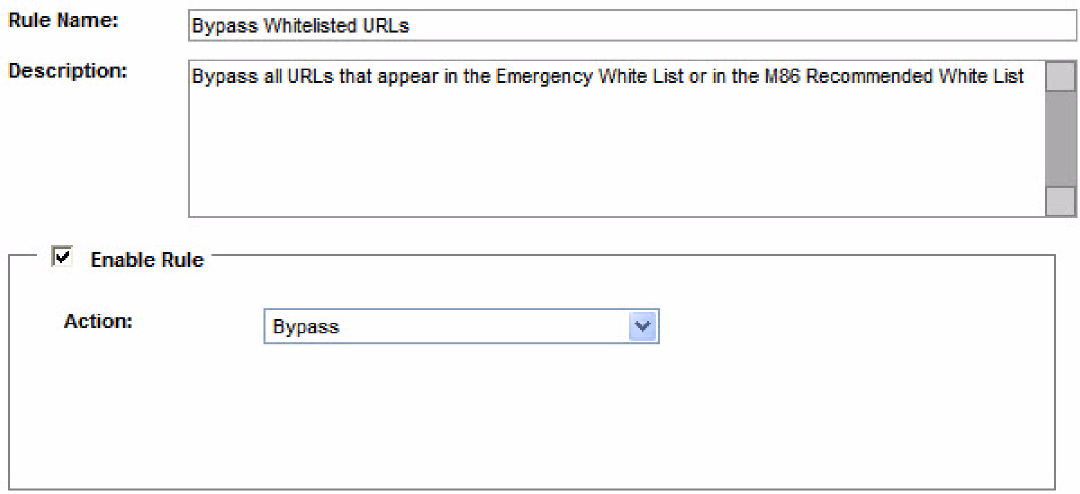
M86 Emergency HTTPS Policy Rules

The M86 Emergency HTTPS Policy consists of two rules:

- Bypass Whitelisted URLs
- Block all HTTPS URLS except White Lists

Bypass Whitelisted URLs

The first rule in the M86 Emergency HTTPS Policy is the **Bypass Whitelisted URLs** rule. This rule allows access to trusted Internet sites which are listed on the Emergency white list and the M86 recommended white list.



Rule Name: Bypass Whitelisted URLs

Description: Bypass all URLs that appear in the Emergency White List or in the M86 Recommended White List

☑ Enable Rule

Action: Bypass

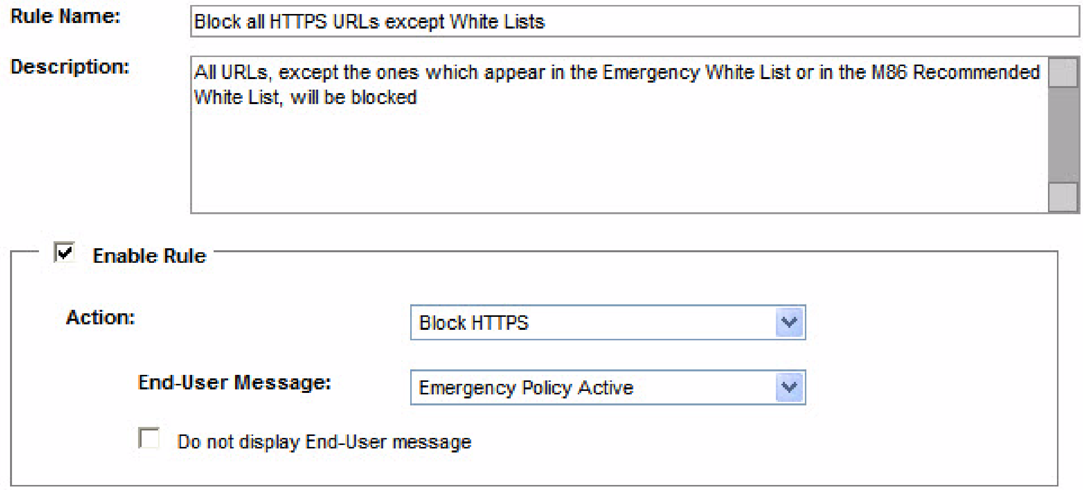
Figure 5-5: Bypass Whitelisted URLs

The following table displays the Rule definitions:

Bypass Whitelisted URLs	
Action	Bypass
Conditions	
URL Lists	M86 Recommended White List, Emergency White List
Bypass Whitelisted URLs	

Block all HTTPS URLS except White Lists

The second rule in the M86 Emergency HTTPS Policy is the **Block all HTTPS URLs except White Lists** rule. This rule blocks access to all URLs that do not appear in the listed white lists.



Rule Name: Block all HTTPS URLs except White Lists

Description: All URLs, except the ones which appear in the Emergency White List or in the M86 Recommended White List, will be blocked

☑ Enable Rule

Action: Block HTTPS

End-User Message: Emergency Policy Active

□ Do not display End-User message

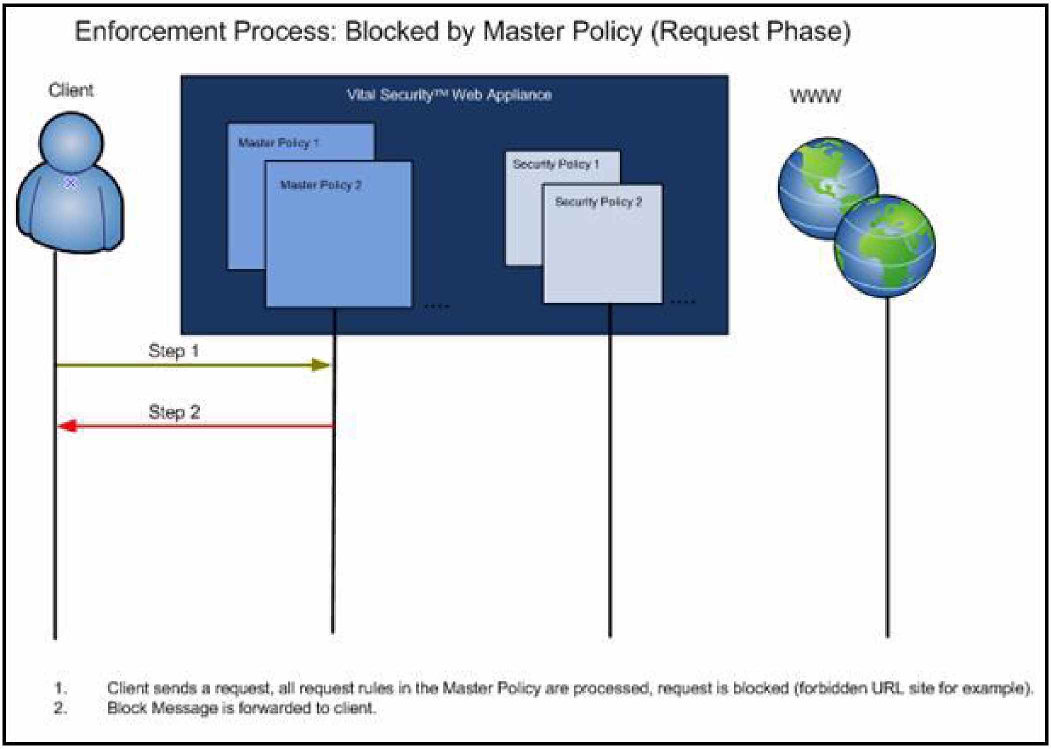
Figure 5-6: Block all HTTPS URLS except White Lists

The following table displays the Rule definitions:

Block all HTTPS URLS except White Lists	
Action	Block HTTPS
End-User Message	Emergency Policy Active
Conditions	
No conditions apply to this rule	

APPENDIX A

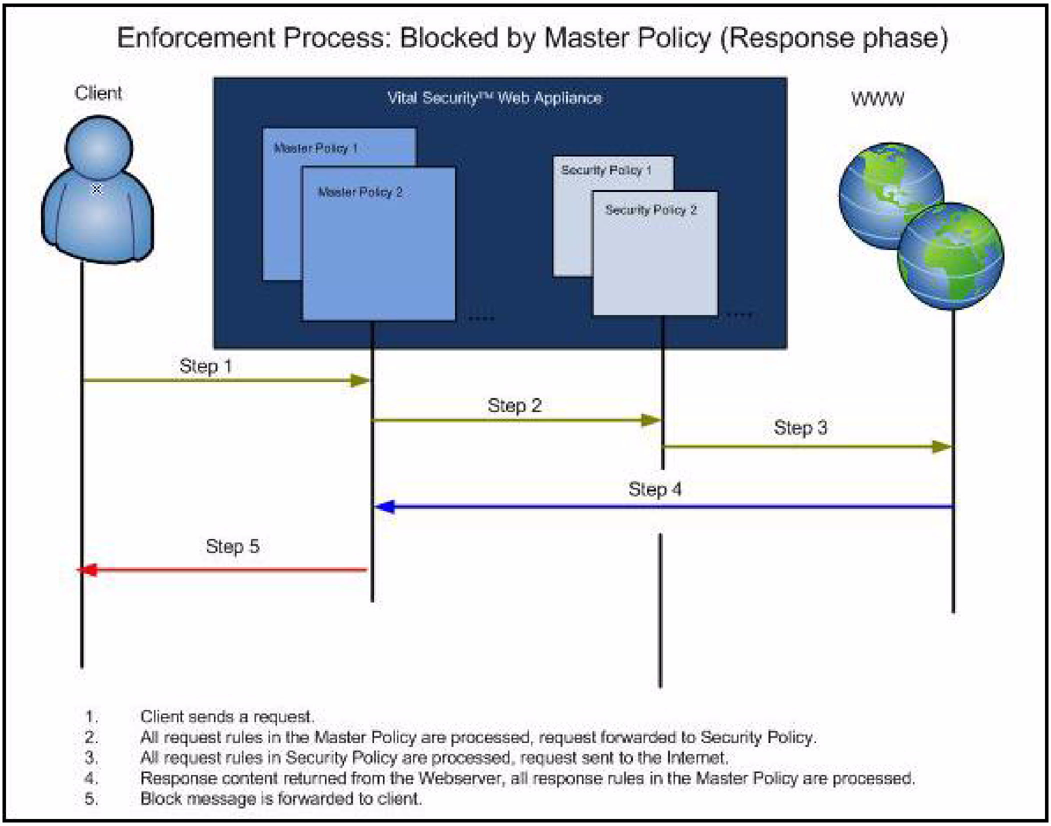
The following diagrams are sample representations of the Master Policy and Security Policy enforcement process.



Enforcement Process: Blocked by Master Policy (Request Phase)

1. Client sends a request, all request rules in the Master Policy are processed, request is blocked (forbidden URL site for example).
2. Block Message is forwarded to client.

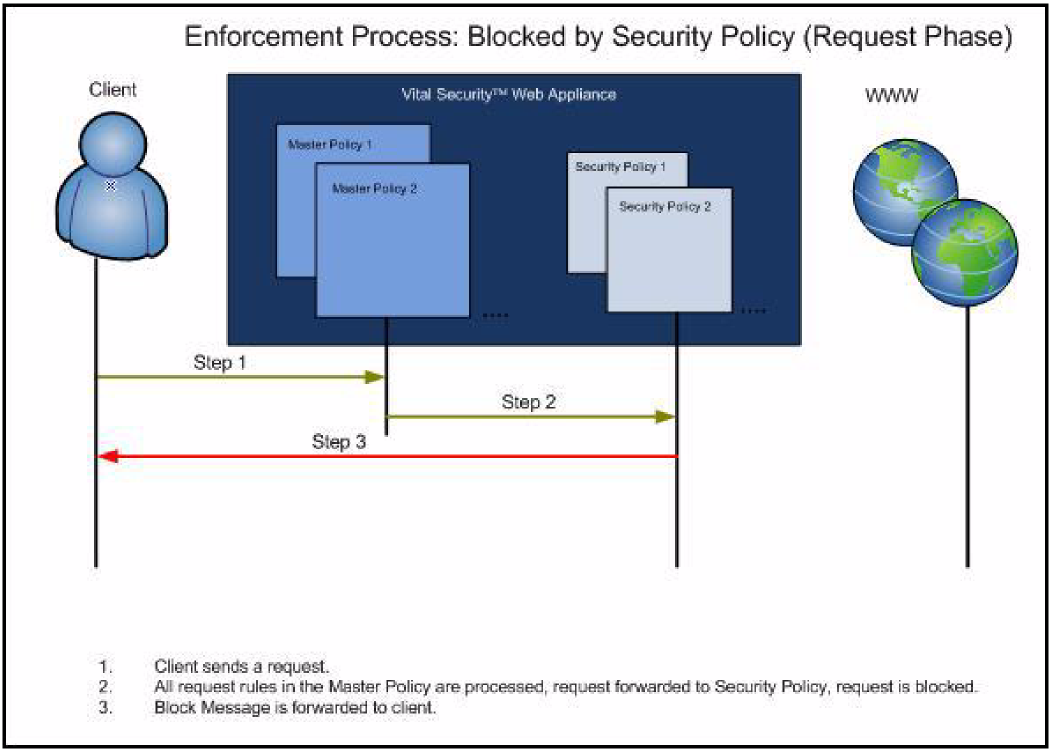
Figure 6-1: Blocked by Master Policy (Request)



Enforcement Process: Blocked by Master Policy (Response phase)

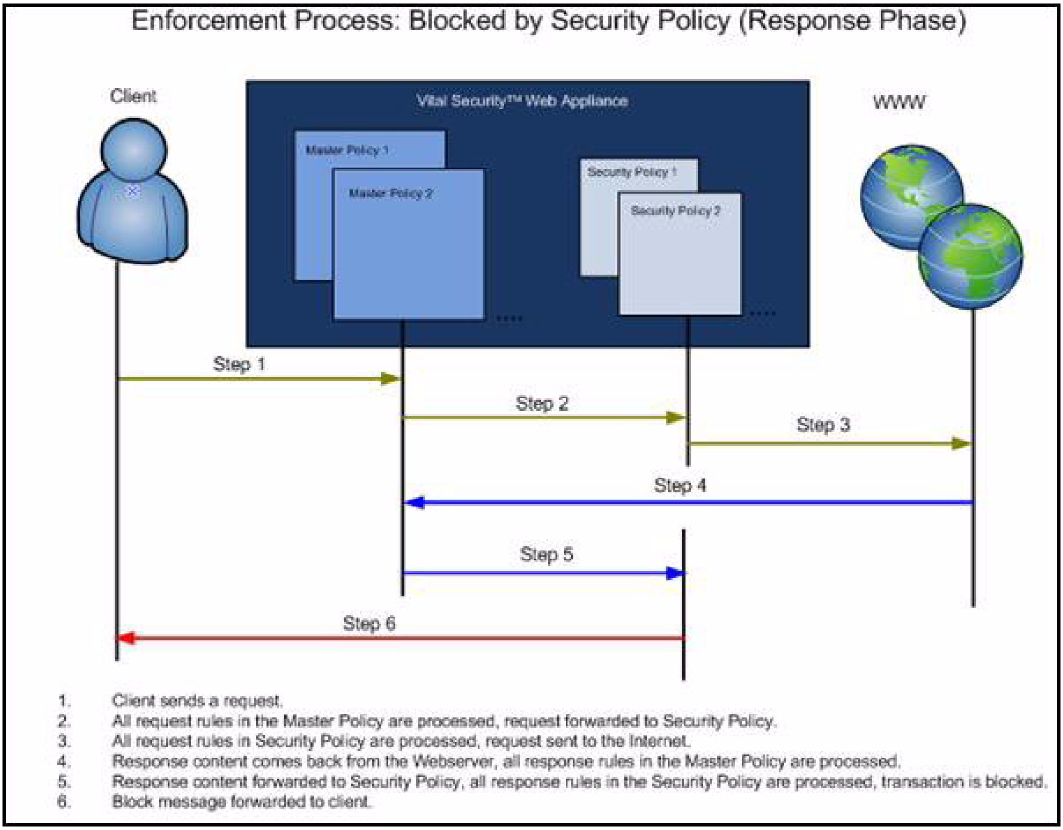
1. Client sends a request.
2. All request rules in the Master Policy are processed, request forwarded to Security Policy.
3. All request rules in Security Policy are processed, request sent to the Internet.
4. Response content returned from the Webserver, all response rules in the Master Policy are processed.
5. Block message is forwarded to client.

Figure 6-2: Blocked by Master Policy (Response)


Enforcement Process: Blocked by Security Policy (Request Phase)
Client
Vital Security™ Web Appliance
WWW
Master Policy 1
Master Policy 2
Security Policy 1
Security Policy 2
Step 1
Step 2
Step 3

1. Client sends a request.
2. All request rules in the Master Policy are processed, request forwarded to Security Policy, request is blocked.
3. Block Message is forwarded to client.

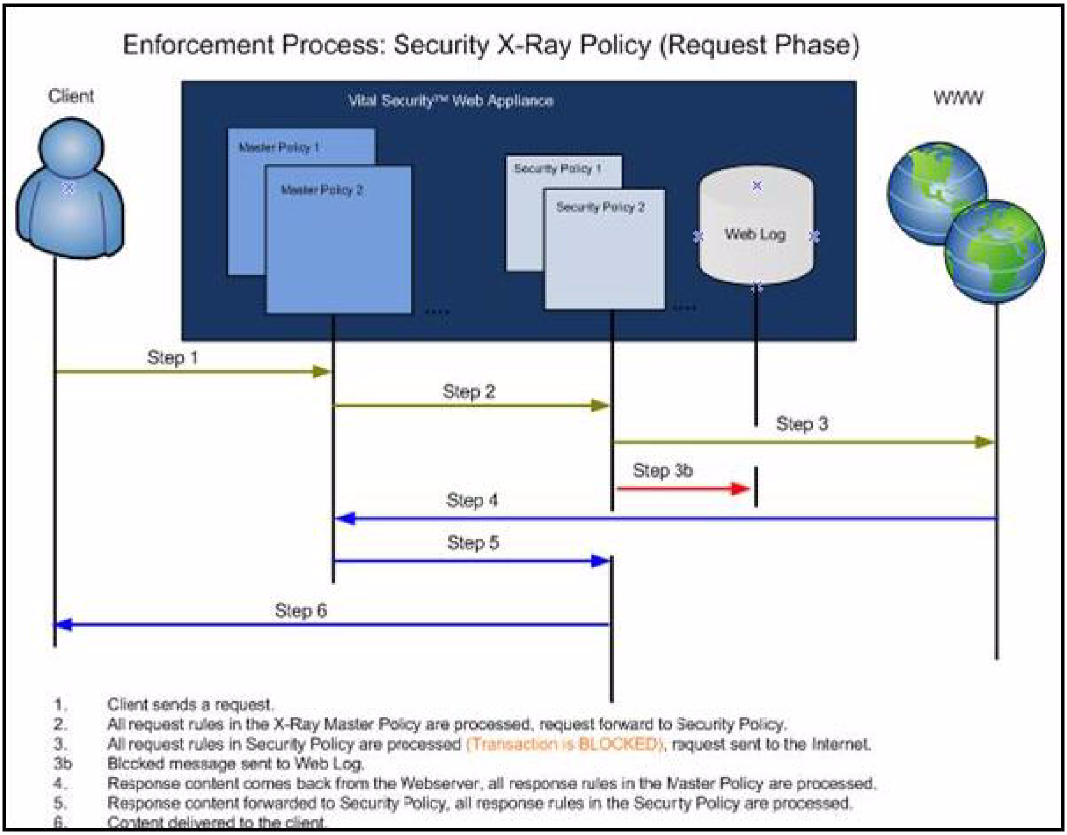
Figure 6-3: Blocked by Security Policy (Request)



Enforcement Process: Blocked by Security Policy (Response Phase)

1. Client sends a request.
2. All request rules in the Master Policy are processed, request forwarded to Security Policy.
3. All request rules in Security Policy are processed, request sent to the Internet.
4. Response content comes back from the Webserver, all response rules in the Master Policy are processed.
5. Response content forwarded to Security Policy, all response rules in the Security Policy are processed, transaction is blocked.
6. Block message forwarded to client.

Figure 6-4: Blocked by Security Policy (Response)



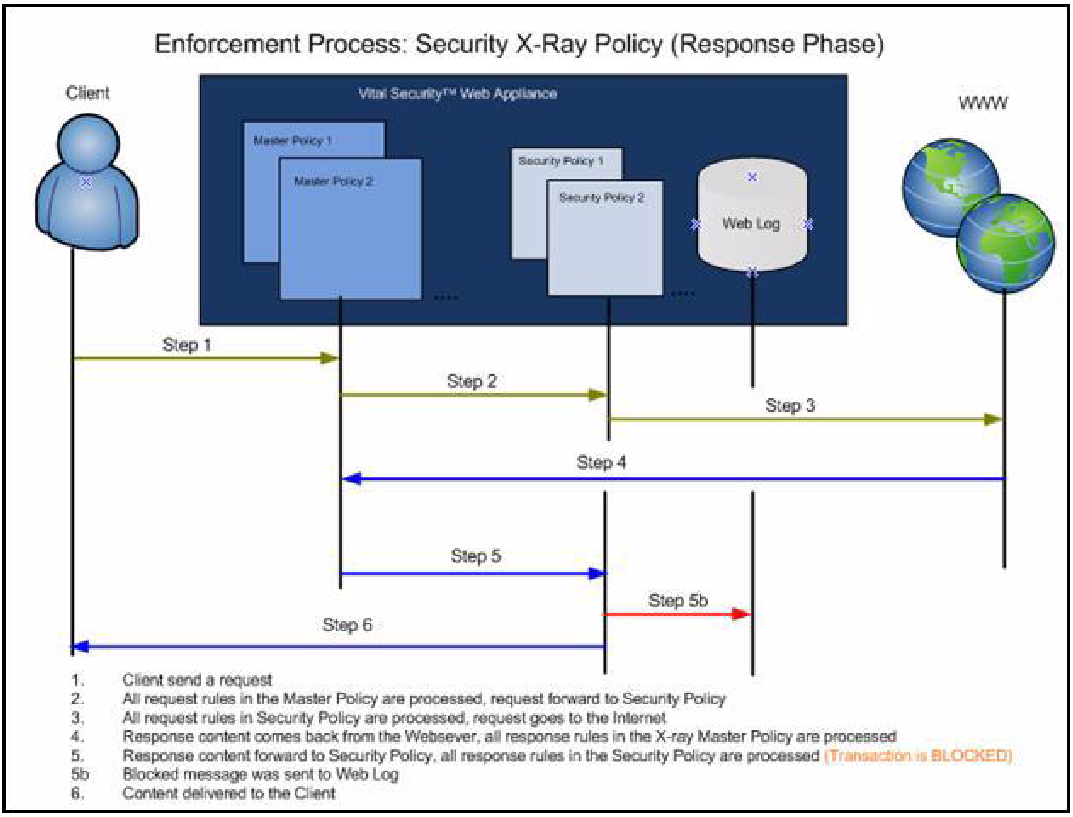
Enforcement Process: Security X-Ray Policy (Request Phase)

1. Client sends a request.
2. All request rules in the X-Ray Master Policy are processed, request forward to Security Policy.
3. All request rules in Security Policy are processed (Transaction is BLOCKED), request sent to the Internet.

3b Blocked message sent to Web Log.

4. Response content comes back from the Webserver, all response rules in the Master Policy are processed.
5. Response content forwarded to Security Policy, all response rules in the Securty Policy are processed.
6. Content delivered to the client.

Figure 6-5: Security X-Ray (Request)



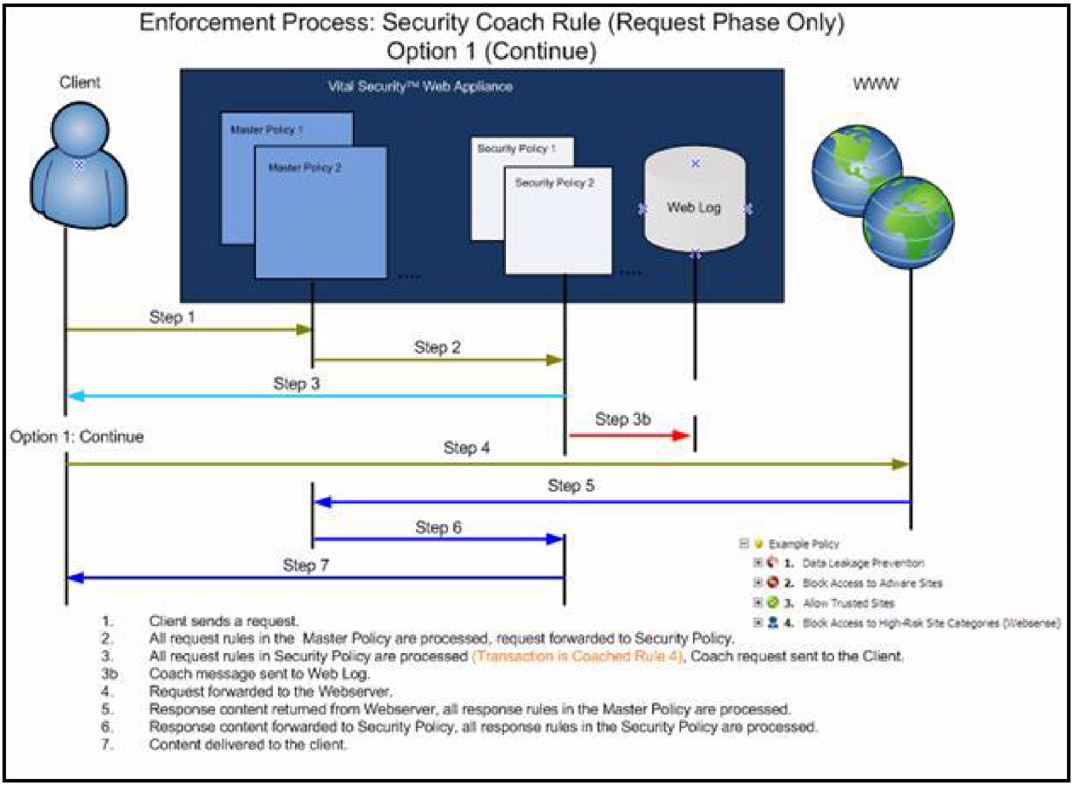
Enforcement Process: Security X-Ray Policy (Response Phase)

1. Client send a request
2. All request rules in the Master Policy are processed, request forward to Security Policy
3. All request rules in Security Policy are processed, request goes to the Internet
4. Response content comes back from the Websever, all response rules in the X-ray Master Policy are processed
5. Response content forward to Security Policy, all response rules in the Security Policy are processed (Transaction is BLOCKED)

5b Blocked message was sent to Web Log

6. Content delivered to the Client

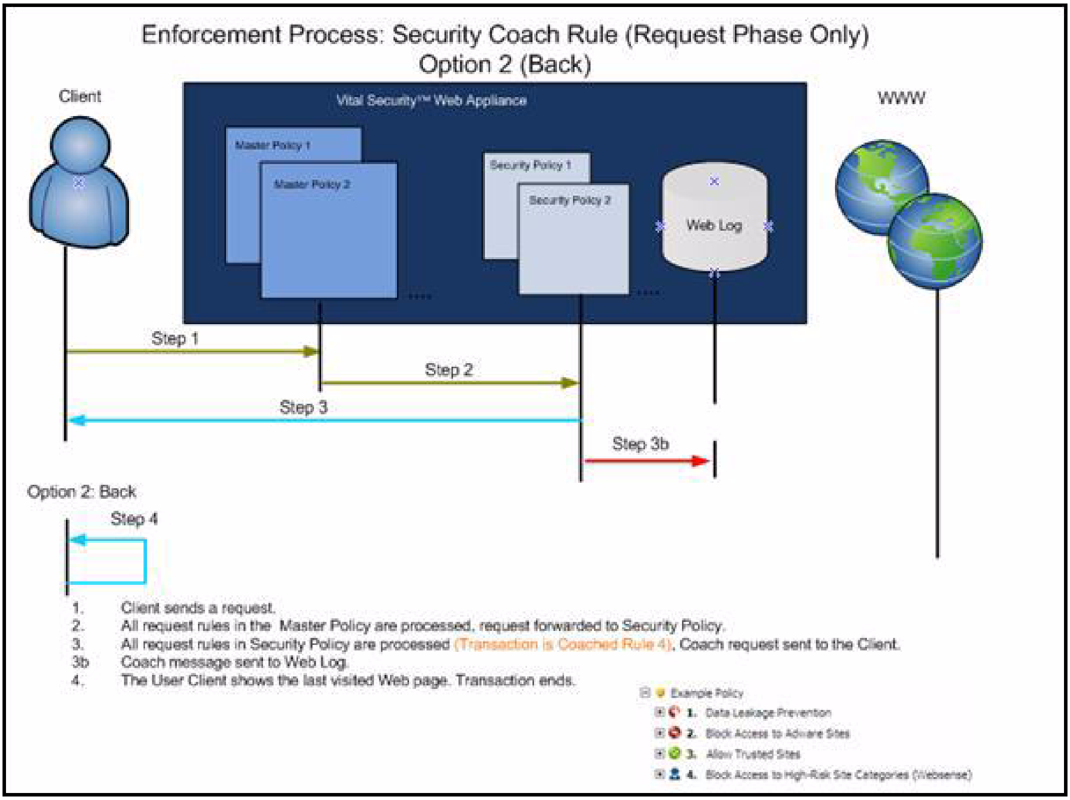
Figure 6-6: Security X-Ray (Response)



Enforcement Process: Security Coach Rule (Request Phase Only)
Option 1 (Continue)

1. Client sends a request.
2. All request rules in the Master Policy are processed, request forwarded to Security Policy.
3. All request rules in Security Policy are processed (Transaction is Coached Rule 4), Coach request sent to the Client.
3b Coach message sent to Web Log.
4. Request forwarded to the Webserver.
5. Response content returned from Webserver, all response rules in the Master Policy are processed.
6. Response content forwarded to Security Policy, all response rules in the Security Policy are processed.
7. Content delivered to the client.

Figure 6-7: Security Coach Rule (Option I)

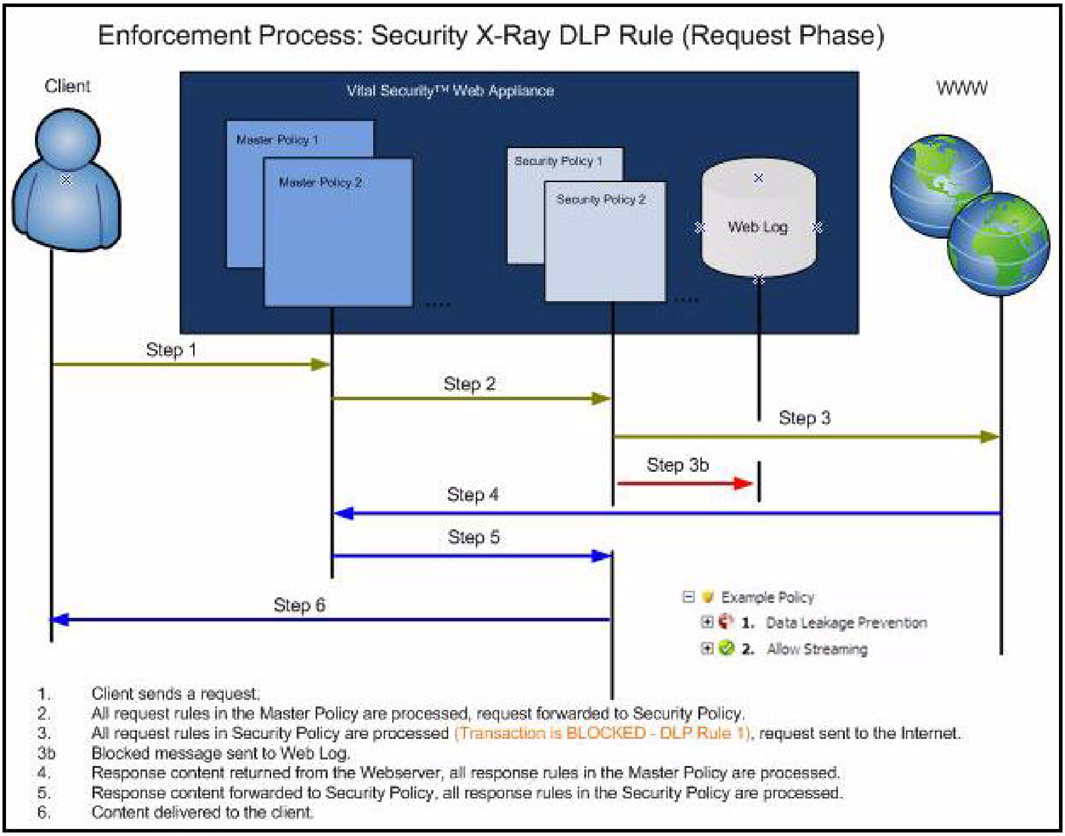


Enforcement Process: Security Coach Rule (Request Phase Only)
Option 2 (Back)

1. Client sends a request.
2. All request rules in the Master Policy are processed, request forwarded to Security Policy.
3. All request rules in Security Policy are processed (Transaction is Coached Rule 4), Coach request sent to the Client.
3b Coach message sent to Web Log.
4. The User Client shows the last visited Web page. Transaction ends.

Example Policy
1. Data Leakage Prevention
2. Block Access to Adware Sites
3. Allow Trusted Sites
4. Block Access to High-Risk Site Categories (Websense)

Figure 6-8: Security Coach Rule (Option II)



Enforcement Process: Security X-Ray DLP Rule (Request Phase)

1. Client sends a request.
2. All request rules in the Master Policy are processed, request forwarded to Security Policy.
3. All request rules in Security Policy are processed (Transaction is BLOCKED - DLP Rule 1), request sent to the Internet.
3b Blocked message sent to Web Log.
4. Response content returned from the Webserver, all response rules in the Master Policy are processed.
5. Response content forwarded to Security Policy, all response rules in the Security Policy are processed.
6. Content delivered to the client.

Figure 6-9: Security X-Ray DLP (Request)