Trend Micro Deep Discovery Analyzer

ICAP Integration Guide with F5

V1.0

Contents

Purpose

- This guide provides step-by-step integration details of Trend Micro Deep Discovery Analyzer with F5 through Internet Content Adaptation Protocol (ICAP).
- There are 2 ways/scenarios to integrate F5 with DDAN ICAP, and both scenarios will be explained in this guide:
  - Scenario One: using ASM policy
  - Scenario Two: using LTM ICAP & Request Adapt profiles

Products Version

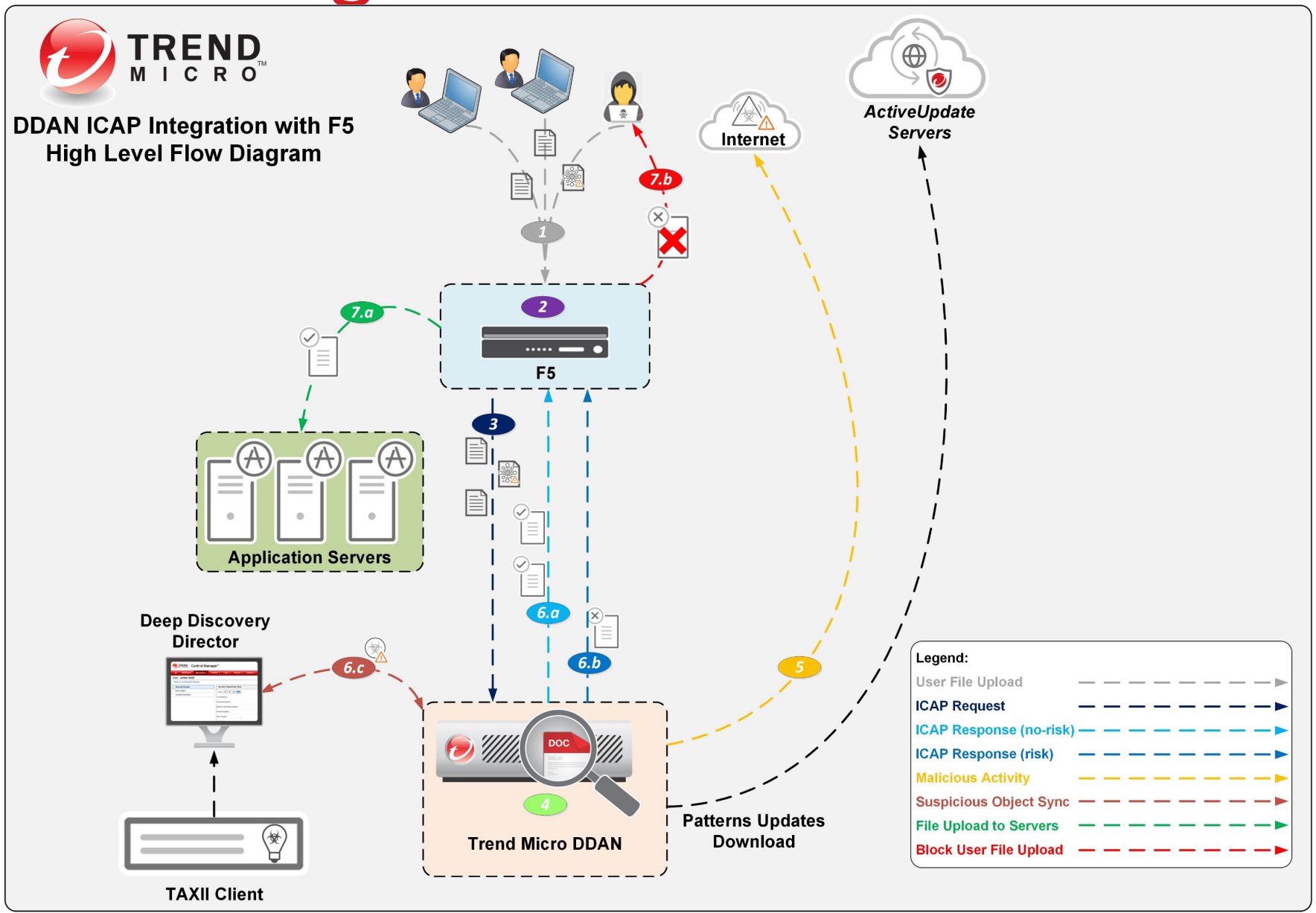
- Deep Discovery Analyzer version:
  - 6.8 or higher

- F5 version:
  - 13.x - 16.x

ICAP Feature Overview

- Deep Discovery Analyzer supports integration with Internet Content Adaptation Protocol (ICAP) clients. After integration, Deep Discovery Analyzer can perform the following functions:
  - Work as an ICAP server that analyzes samples submitted by ICAP clients
  - Control which ICAP clients can submit samples by configuring the ICAP Client list
  - Bypass file scanning based on selected MIME content-types
  - Bypass file scanning based on true file types
  - Bypass URL scanning in RESPMOD mode
  - Scan samples using different scanning modules
  - Filter sample submissions based on the file types that Virtual Analyzer can process

High Level Logical Flow Architecture



Traffic Flow

1. Users send requests for file upload through F5 reverse proxy
2. F5 accepts the requests and process them
3. As an ICAP client, F5 holds the file upload and uses ICAP protocol to submit the file to the Deep Discovery Analyzer for file analysis
4. As an ICAP server, Deep Discovery Analyzer gets the file sample and scans it using different scanning modules
5. During sample processing/scanning, if the sample has any malicious activity that involves connectivity to internet and remote hosts, DDAN will use the dirty line to connect to external destinations.

Based on the scanning analysis result the Deep Discovery Analyzer takes the following actions:

6.a For no-risk samples:

- Deep Discovery Analyzer returns the original message it receives from the ICAP client.
- If the ICAP client supports ICAP 204 No Content, it returns an ICAP 204 No Content response without the original message

6.b For high-risk sample:

- Deep Discovery Analyzer returns an HTTP 403 Forbidden message to the ICAP client
- If X-Virus-ID and X-Infection-Found ICAP headers are enabled, Deep Discovery Analyzer includes these headers within the message

6.c DDAN creates a suspicious object for a sample that is found to have risk, and synchronize the suspicious object details with Deep Discovery Director

Based on the ICAP response received from the Deep Discovery Analyzer, F5 should take one of the following actions:

7.a For no-risk file: F5 forwards the uploaded file to the backend server

7.b For high-risk file: F5 should block the file upload request

DDAN: Enable ICAP

1) Log in to DDAN Configuration utility
2) Go to ***Administration > Integrated Products/Services > ICAP***
3) Select ***Enable ICAP***
4) Type the ICAP port number (the default is 1344)
5) (Optional) In the ***Header Settings*** section, specify how Deep Discovery Analyzer handles ICAP headers
6) (Optional) Under ***Scan Settings***, configure relevant settings
7) (Optional) Under ***ICAP Client List***, Specify the number of Max connections allowed and add ICAP client(s) IP address(es)
8) Click ***Save***

DDAN: Enable ICAP

Integrated Products/Services

Deep Discovery Director | Smart Protection | ICAP | Microsoft Active Directory | SAML Authentication | Syslog

Protocol Settings

If ICAP integration is enabled, Deep Discovery Analyzer automatically slows down Virtual Analyzer throughput to prevent exhaustion of system resources.

- [x] Enable ICAP

ICAP port number: 1344

- [ ] Enable ICAP over SSL

Header Settings

ICAP headers from Deep Discovery Analyzer:

- [x] Enable X-Virus-ID ICAP header
- [x] Enable X-Infection-Found ICAP header
- [x] Enable X-Response-Desc ICAP header

ICAP headers from ICAP clients:

- [x] Enable X-Client-IP ICAP header
- [x] Enable X-Server-IP ICAP header
- [x] Enable X-Authenticated-User ICAP header
- [x] Enable X-Authenticated-Groups ICAP header

Scan Settings

- [x] Bypass URL scanning in RESPMOD mode
- [x] Scan samples using YARA rules
- [x] Scan samples using the selected suspicious objects list
  - (•) Generated suspicious objects list
  - ( ) Synchronized suspicious objects list
- [x] Scan samples using the user-defined suspicious objects list
- [x] Scan samples using the Predictive Machine Learning engine

ICAP Client List

Max connections: 1000

- [ ] Accept scan requests from the following ICAP clients only

+ Add | Delete

	IP Address
	No data to display

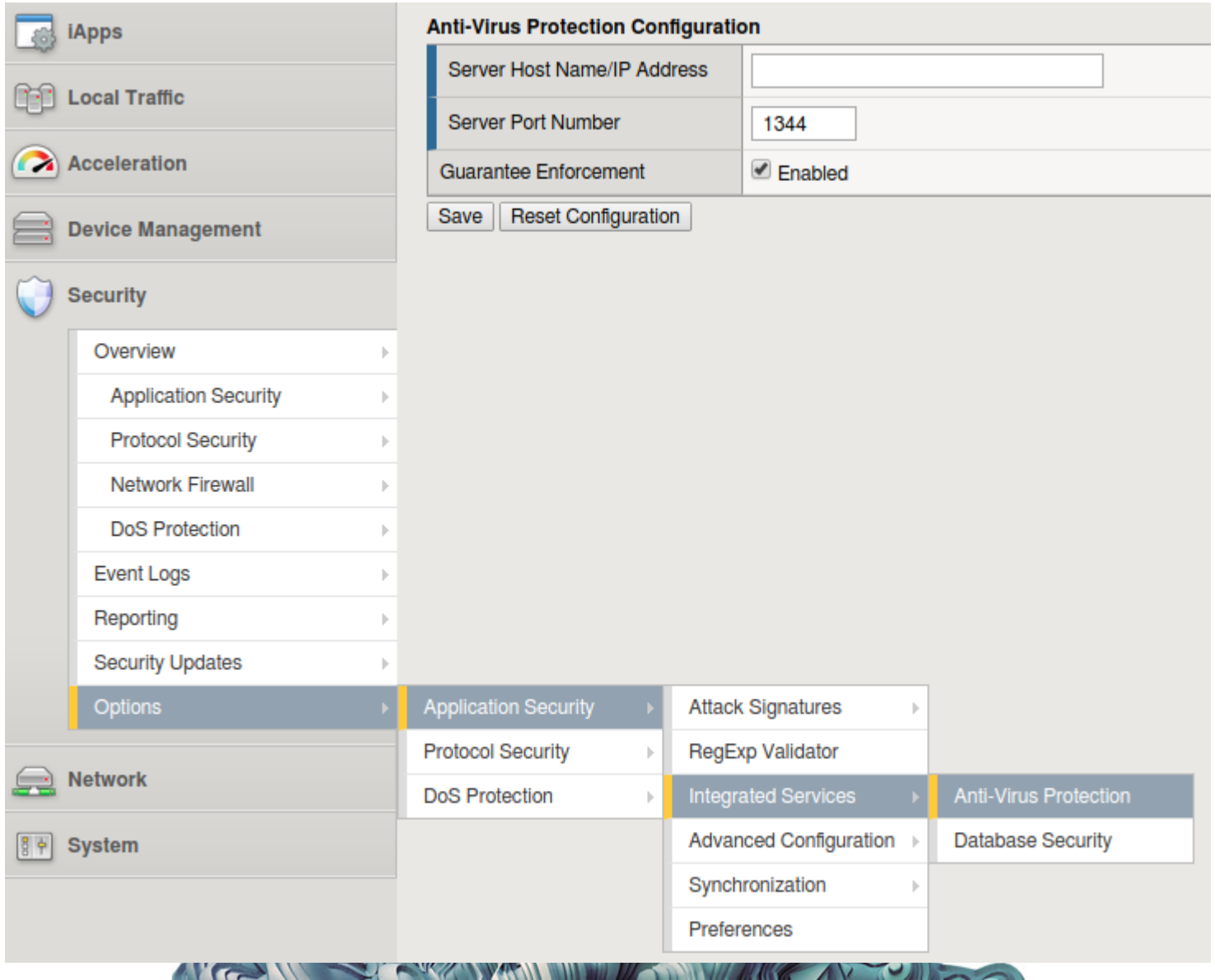
F5 ASM Configuration

- F5 BIG-IP ASM system can be configured to check requests for viruses by configuring the system to connect with an Internet Content Adaptation Protocol (ICAP) server.
- When antivirus protection is configured, the system connects to an external ICAP server and prompts the server to inspect file uploads and attachments for viruses before releasing the content to the pool member.

F5 ASM Step 1: Configuring the ICAP server

1) Log in to F5 Configuration utility
2) Go to ***Security > Options > Application Security > Integrated Services > Anti-Virus Protection***
3) For ***Server Host Name/IP Address***, enter the ICAP server hostname or IP address
4) For ***Server Port Number***, enter the ICAP server port (default is ***1344***)
5) Select the ***Guarantee Enforcement*** check box if you want the system to perform virus checking even if performing checking may slow your web application
6) Select ***Save***
7) To activate the security policy changes immediately, select ***Apply Policy***

F5 ASM Step 1: Configuring the ICAP server



F5 ASM Step 2: Configuring the internal system variables

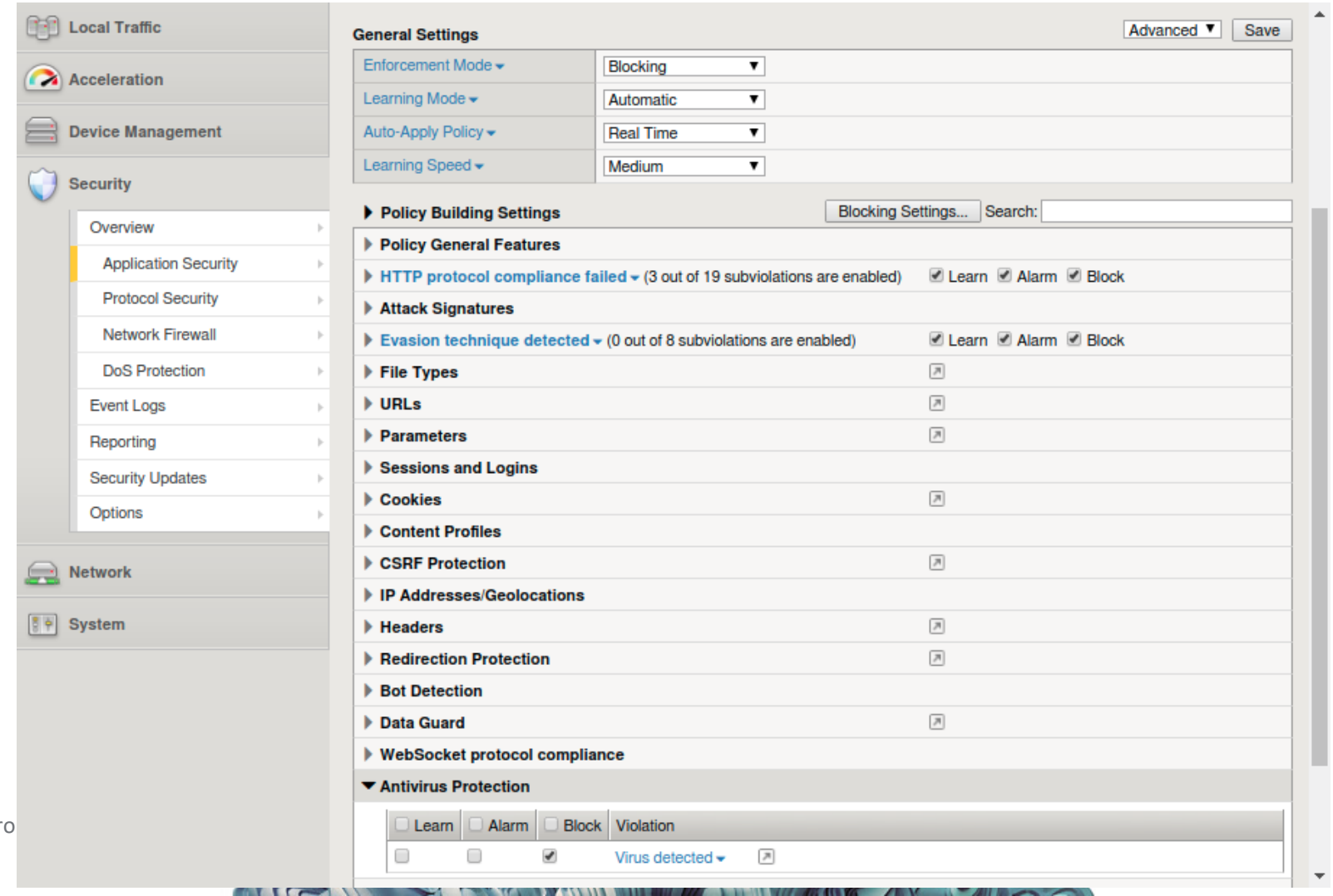
1) Log in to F5 Configuration utility
2) Go to ***Security > Options > Application Security > Advanced Configuration > System Variables***
3) Select the ***icap_uri*** parameter name, enter the URI for the ICAP service in the ***Parameter Value*** setting, which checks requests for viruses by connecting to ICAP server (***/request***)
4) Select the ***virus_header_name*** parameter name, enter the header name used by an antivirus program on an ICAP server in the ***Parameter Value*** setting (***X-Virus-ID, X-Infection-Found, X-Response-Desc***)
5) Select ***Update***

F5 ASM Step 3: Configuring antivirus blocking settings
(for each security policy as needed)

1) Log in to F5 Configuration utility
2) Go to ***Security > Application Security > Policy Building > Learning and Blocking Settings***
3) Set the view to ***Advanced***
4) Expand ***Antivirus*** and select either or both of the ***Alarm*** and ***Block*** check boxes for the Virus Detected violation
5) Select ***Save***
6) To activate the security policy changes immediately, select ***Apply Policy***

F5 ASM Step 3: Configuring antivirus blocking settings

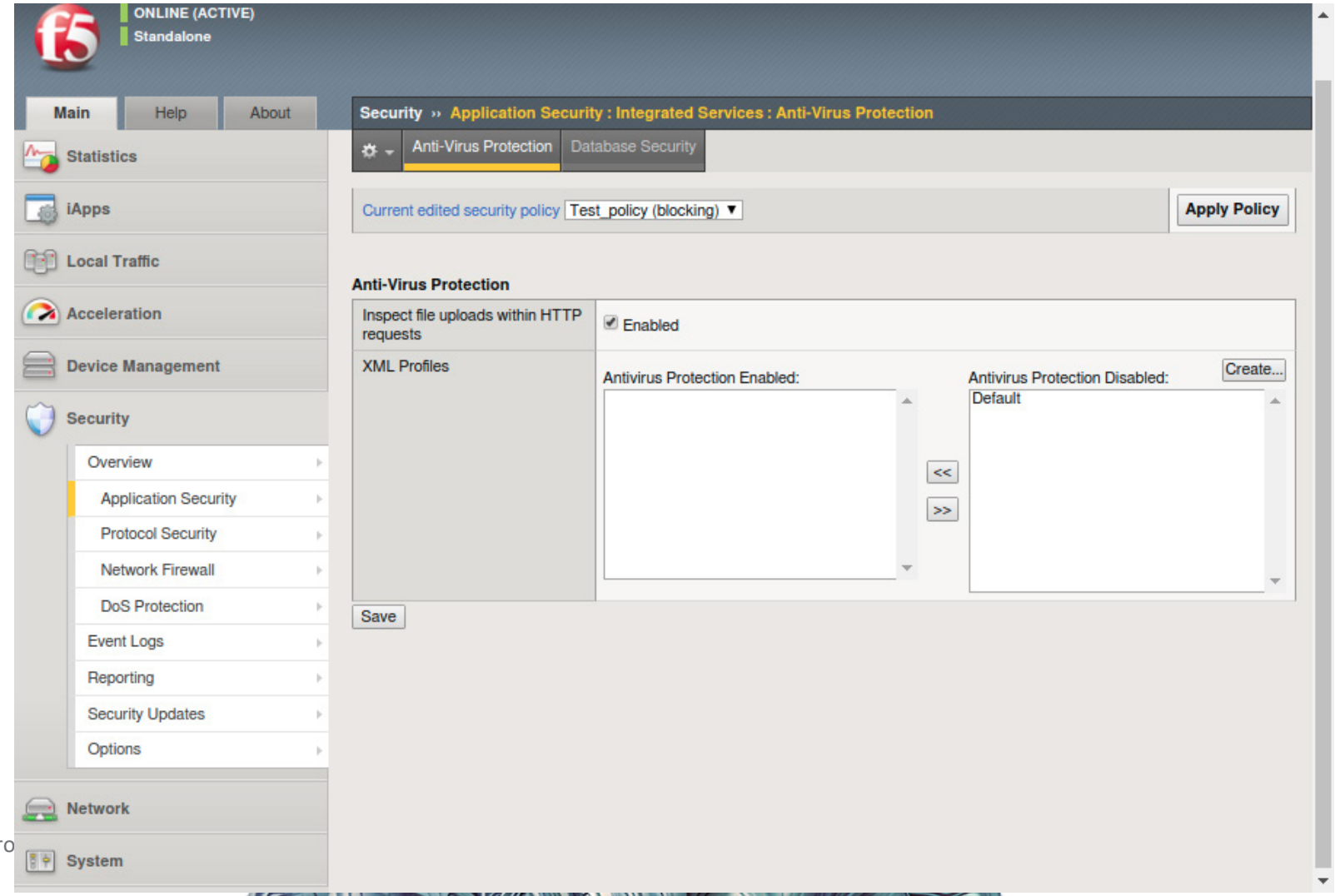
(for each security policy as needed)



F5 ASM Step 4: Configuring antivirus scanning for HTTP file uploads and SOAP attachments

1) Log in to F5 Configuration utility
2) Go to ***Security > Application Security > Integrated Services > Anti-Virus Protection***
3) Select the ***Inspect file uploads within HTTP requests*** check box.
4) To perform antivirus scanning on SOAP attachments, move the relevant XML profiles from the Antivirus Protection Disabled list to the Antivirus Protection Enabled list
5) Select ***Save***
6) To activate the security policy changes immediately, select ***Apply Policy***

F5 ASM Step 4: Configuring antivirus scanning for HTTP file uploads and SOAP attachments

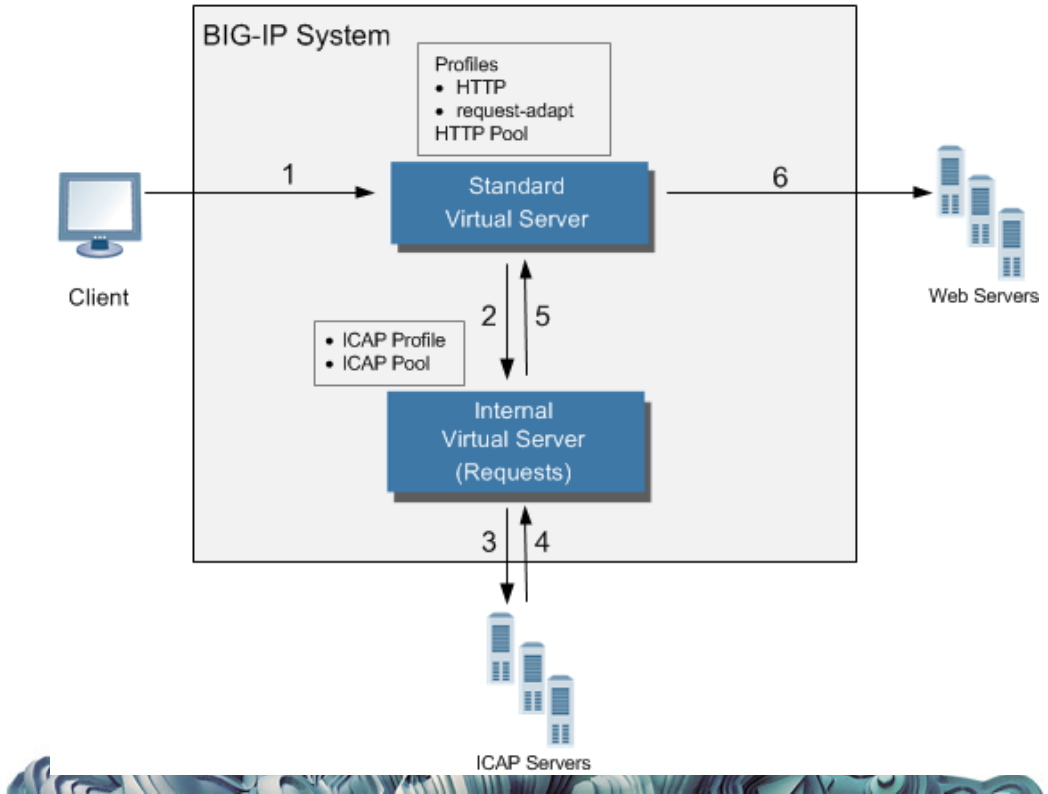


F5 LTM Configuration

- F5 LTM system can be configured to use content adaptation feature for adapting HTTP requests. With this feature, a virtual server can conditionally forward HTTP requests to a pool of ICAP servers, before sending the request to a web server.
- The HTTP virtual server accepts each client request in the normal way, but before load balancing the request to the pool of web servers, the virtual server forwards the HTTP request to a special internal virtual server.

F5 LTM Configuration

- The internal virtual server receives the HTTP request from the standard virtual server, and load balances the request to a pool of ICAP servers. After the ICAP server modifies the request, the BIG-IP system sends the request to the appropriate web server for processing.



F5 LTM Step 1: Configuring ICAP profile

1) Log in to F5 Configuration utility
2) Go to ***Local Traffic > Profiles > Services > ICAP***
3) Click ***Create***
4) In the ***Name*** filed, type a unique name for the profile
5) For the ***Parent Profile*** setting, retain the default value, ***icap***
6) On the right side of the screen, select the ***Custom*** check box
7) In the ***URI*** field, type a URI in this format:

   icap://ddan_host_name:port/request

   (default port is ***1344***)

F5 LTM Step 1: Configuring ICAP profile

8) In the ***Preview Length*** field, type a length or retain the default value ***0***
9) In the ***Header From*** field, type a value for the ***From:*** ICAP Header
10) In the ***Host*** field, type a value for the ***Host:*** ICAP Header
11) In the ***Referer*** field, type a value for the ***Referer:*** ICAP Header
12) In the ***User Agent*** field, type a value for the ***User-Agent:*** ICAP Header
13) Click ***Finished***

F5 LTM Step 2: Configuring a pool of ICAP servers

1) Log in to F5 Configuration utility
2) Go to ***Local Traffic > Pools***
3) Click ***Create***
4) In the ***Name*** filed, type a unique name for the pool
5) For the ***Health Monitors*** setting, from the ***Available*** list, select ***http*** monitor and move the monitor to the ***Active*** list
6) From the ***Load Balancing Method*** list, select how the system distributes traffic to members of this pool, the default is ***Round Robin***

F5 LTM Step 2: Configuring a pool of ICAP servers

7) Using the ***New Members*** setting, add each resource that you want to include in the pool:
   a) (Optional) In the ***Node Name*** field, type a name for the node portion of the pool member.
   b) In the ***Address*** field, type an IP address.
   c) In the ***Service Port*** field, type a port number, or select a service name from the list.
   d) (Optional) In the ***Priority*** field, type a priority number.
   e) Click ***Add***
8) Click ***Finish***

F5 LTM Step 3: Configuring an internal virtual server

1) Log in to F5 Configuration utility
2) Go to ***Local Traffic > Virtual Servers***
3) Click ***Create***
4) In the ***Name*** filed, type a unique name for the virtual server
5) In the ***Type*** list, select ***Internal***
6) For the ***State*** setting, verify that the value is set to ***Enabled***
7) From the ***Configuration*** list, select ***Advanced***
8) From the ***ICAP*** profile list, select the ICAP profile that you created
9) From the ***Default Pool*** list, select the pool of ICAP servers that you created
10) Click ***Finished***

F5 LTM Step 4: Configuring a request adapt profile

1) Log in to F5 Configuration utility
2) Go to ***Local Traffic > Profiles > Services > Request Adapt***
3) Click ***Create***
4) In the ***Name*** filed, type a unique name for the profile
5) For the ***Parent Profile*** setting, retain the default value, ***requestadapt***
6) On the right-side of the screen, clear the ***Custom*** check box
7) For the ***Enabled*** settings, retain the default value, ***Enabled***
8) From the ***Internal Virtual Name*** list, select the name of the internal virtual server that you created

F5 LTM Step 4: Configuring a request adapt profile

9) In the ***Preview Size*** field, type a numeric value, this specifies the maximum size of the preview buffer
10) In the ***Timeout*** field, type a numeric value in seconds, use ***0*** to disable it
11) From the ***Service Down Action*** list, select an action for the system to take if the internal virtual server returns an error:
    a) Select ***Ignore*** to ignore the error and send the unmodified HTTP request to the HTTP web server
    b) Select ***Drop*** to drop the connection
    c) Select ***Reset*** to reset the connection
12) Click ***Finished***

F5 LTM Step 5: Configuring a virtual server with request adapt profile

- After creating the Request Adapt profile, it can be used by a standard HTTP/HTTPs virtual server to forward an HTTP request to an internal virtual server for ICAP traffic
  1) Log in to F5 Configuration utility
  2) Go to **Local Traffic > Virtual Servers** and select a virtual server to edit
  3) From the **Configuration** list, select **Advanced**
  4) From the ***Request Adapt Profile*** list, select the name of the Request Adapt profile that is created
  5) Click ***Finished***

References

- **Deep Discovery Analyzer:**
  - ICAP: https://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer-71/administration/integrated-productss/icap-tab.aspx
  - ICAP Settings: https://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer-71/administration/integrated-productss/icap-tab/configuring-icap-set.aspx
  - ICAP Header Responses: https://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer-71/virtual-analyzer_001/submissions/icap-submissions-/icap-header-response.aspx
- **F5:**
  - ASM: https://support.f5.com/csp/article/K70941653
  - LTM: https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-13-0-0/9.html

End.