Firepower Data Path Troubleshooting Phase 6: Active Authentication

Contents

Introduction

This article is part of a series of articles which explain how to systematically troubleshoot the data path on Firepower systems to determine whether components of Firepower may be affecting traffic. Please refer to the Overview article for information about the architecture of Firepower platforms and links to the other Data Path Troubleshooting articles.

This article covers the sixth stage of Firepower data path troubleshooting, the Active Authentication feature.

Prerequisites

- This article pertains to all of the currently supported Firepower platforms
- The Firepower device must be running in Routed Mode

Troubleshooting the Active Authentication Phase

When trying to determine if an issue is caused by identity, it is important to understand what traffic this feature can impact. The only features in identity itself that can cause traffic interuptions are the ones related to active authentication. Passive authentication cannot cause traffic to be dropped unexpectedly. It is important to understand that only HTTP(S) traffic is impacted by active authentication. If other traffic is impacted because identity is not working then this is more likely

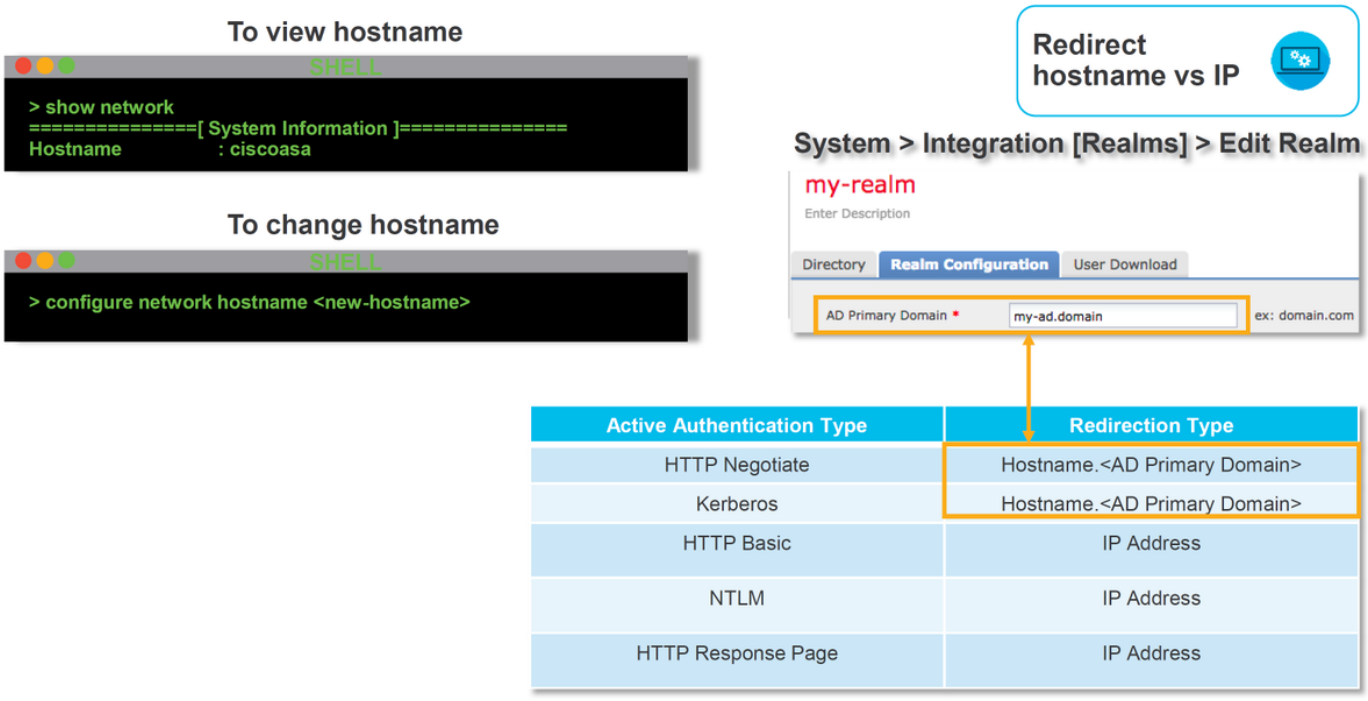
because the policy uses users/groups to allow/block traffic, so when the identity feature can't identify users, unexpected things can occur, but it depends on the device Access Control policy and Identity Policy. The troubleshooting in this section walks through issues related to active authentication only.

Verify the Redirect Method

The active authentication features involve the Firepower device running an HTTP server. When traffic matches an Identity Policy rule which contains an Active Authentication action, Firepower sends a 307 (temporary redirect) packet into the session, so as to redirect clients to its captive portal server.

There are currently five different types of active authentication. Two redirects to a hostname which consists of the sensor's hostname and the Active Directory primary domain tied to the realm, and three redirects to the IP address of the interface on the Firepower device which is performing the captive portal redirect.

If something goes wrong in the redirect process, the session can break as the site isn't available. This is why it is important to understand how the redirection is operating in the running configuration. The chart below helps to understand this configuration aspect.



Active Authentication Type	Redirection Type
HTTP Negotiate	Hostname.<AD Primary Domain>
Kerberos	Hostname.<AD Primary Domain>
HTTP Basic	IP Address
NTLM	IP Address
HTTP Response Page	IP Address

If active authentication is redirecting to the hostname, it would be redirecting the clients to **ciscoasa.my-ad.domain:<port_used_for_captive_portal>**

Generate Packet Captures

Collecting packet captures is the most important part of troubleshooting active authentication issues. The packet captures take place on two interfaces:

1. The interface on the Firepower device which the traffic is ingressing when identity/authentication is being performed In the example below, the **inside** interface is used

2. The internal tunnel interface which Firepower uses for redirection to the HTTPS server - **tun1**
   This interface is used to redirect traffic to the captive portalThe IP addresses in the traffic are changed back to the originals upon egress

```
> capture ins_ntlm interface inside buffer 1000000 match tcp host 192.168.62.31 any
> expert

# tcpdump -i tun1 -s 1518 -w /var/common/ntlm_tun.pcap

[Test authentication and then stop captures]

# ^C
> capture ins_ntlm stop

> copy /noconfirm /pcap capture:ins_ntlm ins_ntlm.pcap
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
748 packets copied in 0.40 secs


[ File will be copied here: /mnt/disk0/ins_ntlm.pcap ]
```

The two captures are initiated, the interesting traffic is run through the Firepower device, then the captures are stopped.

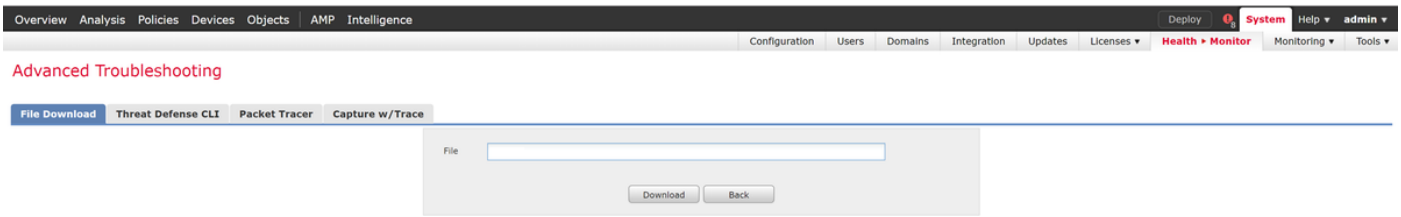
Notice that the inside interface packet capture file, "ins_ntlm", is copied to the **/mnt/disk0** directory. It can then be copied to the /var/common directory so as to be downloaded off of the device (**/ngfw/var/common** on all FTD platforms):

```
> expert
# copy /mnt/disk0/<pcap_file> /var/common/
```

The packet capture files can then be copied off of the Firepower device from the > prompt using the directions in this article.

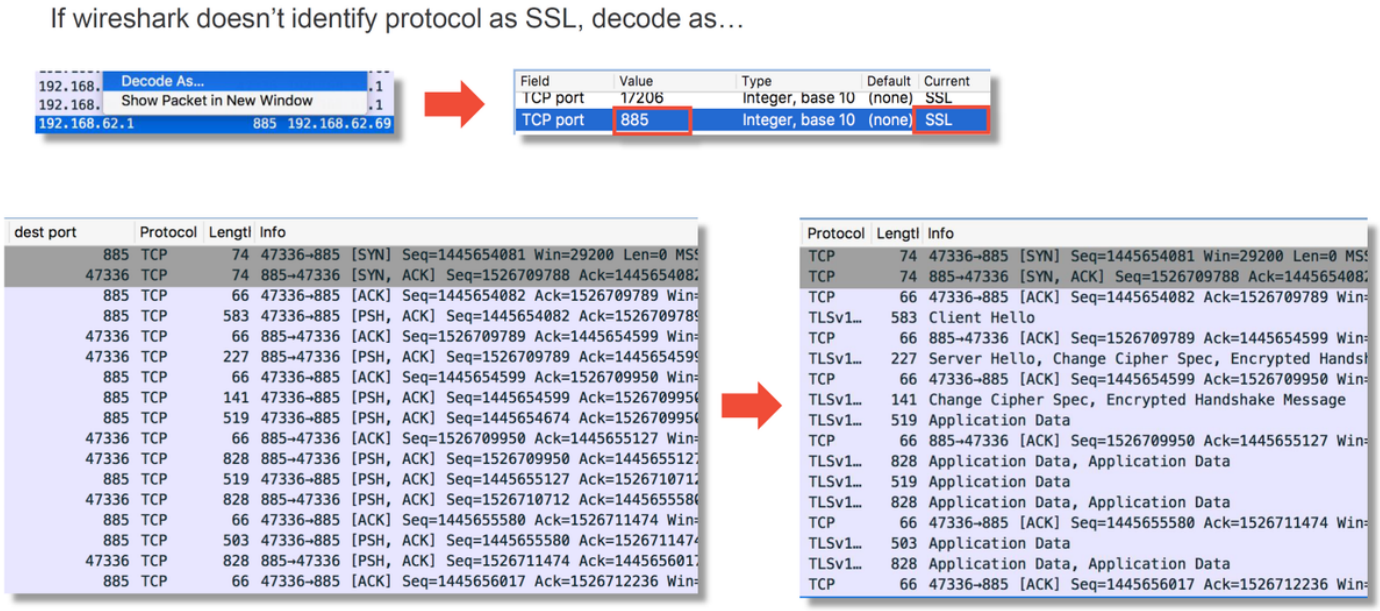
Alternatively, there is n option on the Firepower Management Center (FMC) in Firepower version 6.2.0 and greater. To access this utility on the FMC, navigate to **Devices > Device Management**.

Then, click on the  icon next to the device in question, followed by **Advanced Troubleshooting > File Download**. You can then enter the name of a file in question and click Download.

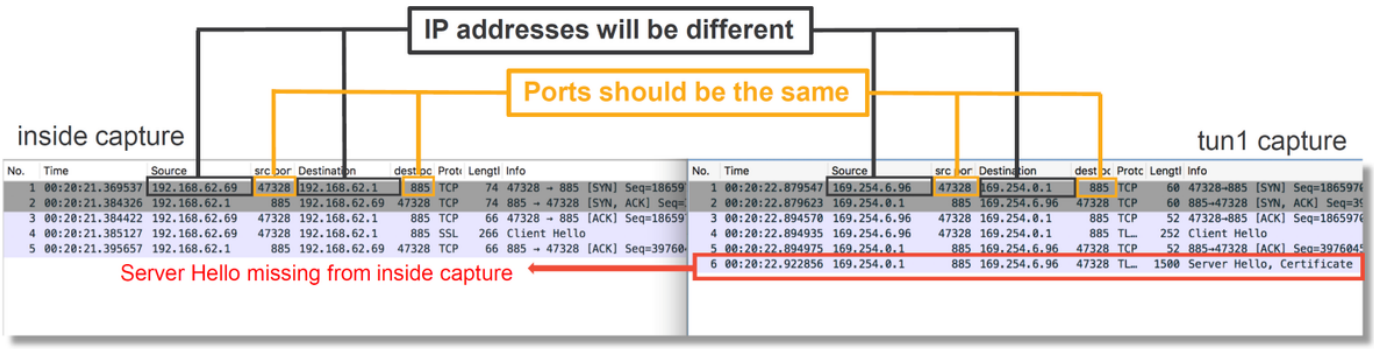


Packet Capture (PCAP) File Analysis

PCAP analysis in Wireshark can be performed to help identify the issue within the active authentication operations. Since a non-standard port is used in the captive portal configuration (**885** by default), Wireshark needs to be configured to decode the traffic like SSL.



The inside interface capture and the tunnel interface capture should be compared. The best way to identify the session in question in both PCAP files is to locate the unique source port since the IP addresses is different.



In the example above, notice that the server hello packet is missing from the inside interface capture. This means that it never made it back to the client. It is possible that the packet was dropped by snort, or possibly due to a defect or misconfiguration.

Note: Snort inspects its own captive portal traffic so as to prevent any HTTP exploits.

Decrypting the Encrypted Stream

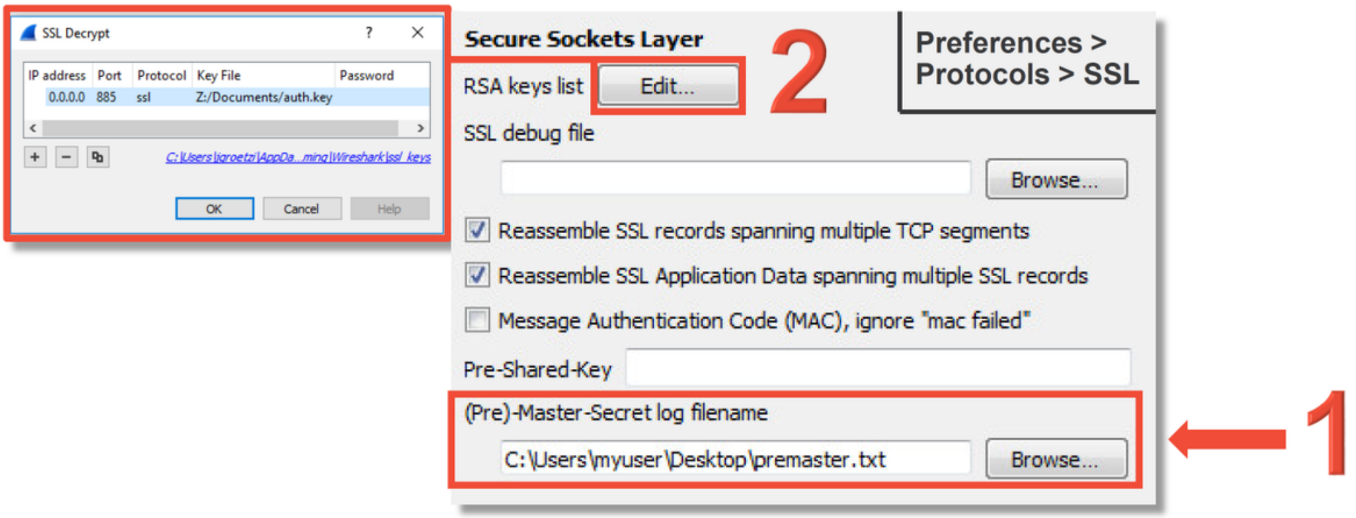
If the problem is not in the SSL stack, it may be beneficial to decrypt the data in the PCAP file so as to see the HTTP stream. There are two methods by which this can be accomplished.

1. Set an environment variable in Windows (more secure - recommended) This method involves creating a premaster secret file. This can be done with the following command (run from the windows command terminal): **setx SSLKEYIOGFILE "%HOMEPATH%\Desktop\premaster.txt"**A private session can then be opened in Firefox, in which you can browse to the site in question, which uses SSL.The symmetric key is then logged to the file specified in the command from step 1 above.Wireshark can use the file to

decrypt using the symmetric key (see diagram below).

2. Use the RSA private key (less secure, unless using a test certificate and user) The private key to be used is the one used for the captive portal certificateThis doesn't work for non-RSA (like Elliptic Curve) or anything ephemeral (Diffie-Hellman, for example)

Caution: If method 2 is used, do not provide Cisco Technical Assistance Center (TAC) your private key. A temporary test certificate and key can be used, however. A test user should also be used in testing.



Viewing the Decrypted PCAP File

In the example below, a PCAP file has been decrypted. It shows that NTLM is being used as the active authentication method.

```
HTTP/1.1 401 Unauthorized
Date: Thu, 25 May 2017 00:21:42 GMT
Server: Apache
WWW-Authenticate: NTLM
TlRMTVNTUAACAAAACgAKADgAAAAFgomiqq2eSri57HcAAAAAAAAAAKgAqABCAAAABgOAJQAAAA9KAEcALQBBAEQAAgAKAEoARwAtAEEARAABA
BgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQABAAYAGoAZwAtAGEAZAAuAGYAdQBsAHQAbwBuAAMAMgBqAGcALQB3AGkAbgAyADAAMQAyAGEAZA
AuAGoAZwAtAGEAZAAuAGYAdQBsAHQAbwBuAAUAGABqAGcALQBhAGQALgBmAHUAbAB0AG8AbgAHAAgApNC54uzU0gEAAAAA
Content-Length: 381
Keep-Alive: timeout=10, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</body></html>
GET /x.auth?s=9n1DsDbFKVcS%2Fj71hez1nLYh%2F5qfEzgMgJd%2FdQEyyRs%3D&u=http%3A%2F%2Fwww.cisco.com%2F HTTP/1.1
Host: 192.168.62.1:885
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Authorization: NTLM
TlRMTVNTUAADAAAAGAAYAIgAAABSAVIBoAAAAAAAAABYAAAAGgAaAFgAAAAWABYAcgAAAAAAAADyAQAABYKIogYBsB0AAAAPI6ZJFPLSnhAOl
XwHPmh3AkEAZABtAGkAbgBpAHMAdAByAGEAdABvAHIASgBHAFIATwBFAFQAWgBJAC0AUABDAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAANrNXy
RPxPwOAPpWmWMvfnEBAQAAAAAAAKTQueLs1NIBEBvFTnBWA0sAAAAAAgAKAEoARwAtAEEARAABABgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQ
ABAAYAGoAZwAtAGEAZAAuAGYAdQBsAHQAbwBuAAMAMgBqAGcALQB3AGkAbgAyADAAMQAyAGEAZAAuAGoAZwAtAGEAZAAuAGYAdQBsAHQAbwBu
AAUAGABqAGcALQBhAGQALgBmAHUAbAB0AG8AbgAHAAgApNC54uzU0gEGAAQAAgAAAAgAMAAwAAAAAAAAAAAEAAAAAIAAAGnon72xFiGN/nI
+x5HgnhIcuVFrNJLs2tch8vxbrx90KABAAAJYqfNSUhlBA9xs44bOV4AkAIgBIAFQAVABQAC8AMQA5ADIALgAxADYAOAAuADYAMgAuADEAAAA
AAAAAAAAAAAAA

HTTP/1.1 307 Temporary Redirect
Date: Thu, 25 May 2017 00:21:42 GMT
Server: Apache
Location: http://www.cisco.com/
Content-Length: 231
Keep-Alive: timeout=10, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

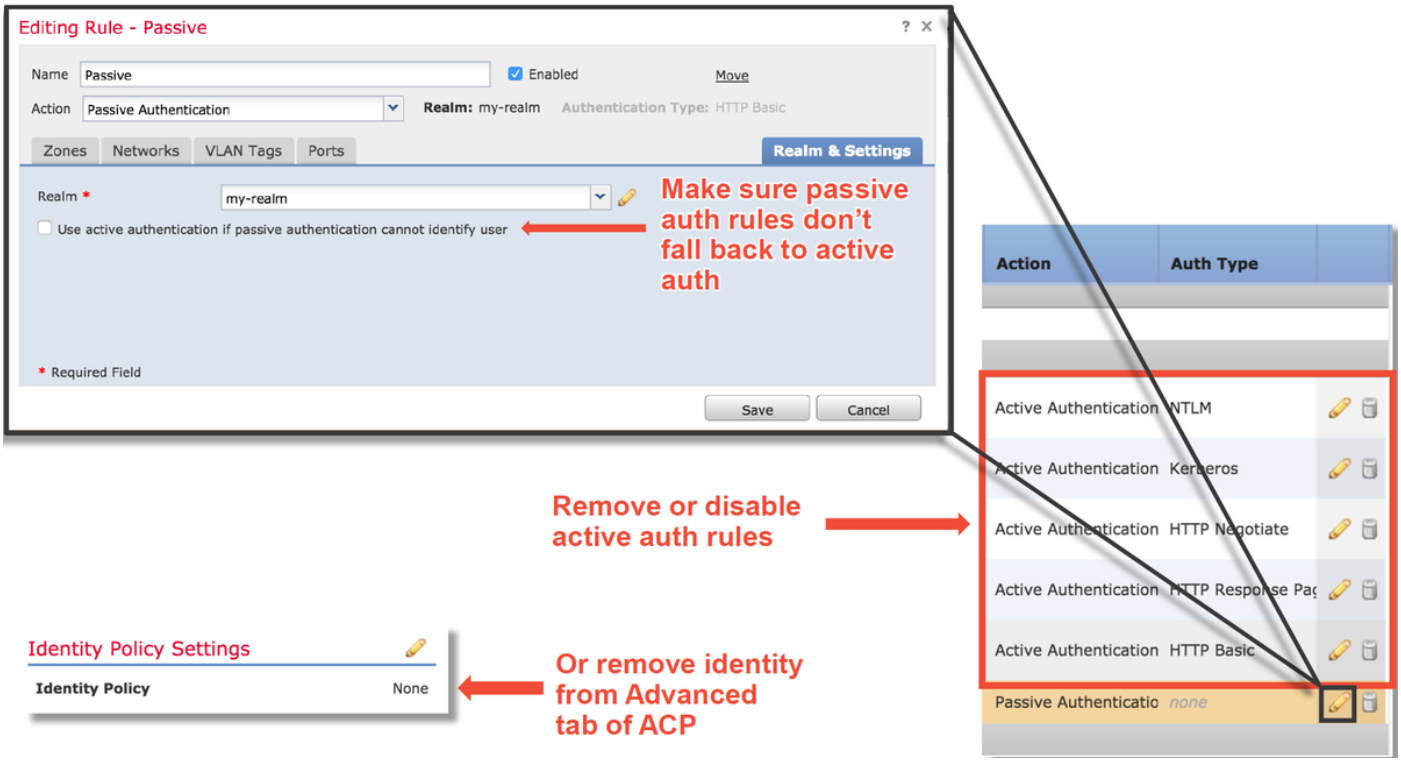
After NTLM authorization takes place, the client is redirected back to the original session, so that it can reach its intended destination, which is http://www.cisco.com.

Mitigation Steps

Switch to Passive Authentication Only

When used in an Identity Policy, Active Authentication has the ability to drop allowed (HTTP(s) traffic only), if something goes wrong in the redirect process. A quick mitigation step is to disable any rule within the Identity Policy with the action of **Active Authentication**.

Also, make sure that any rules with 'Passive Authentication' as action do not have the 'Use active authentication if passive authentication cannot identify user' option checked.



Data to Provide to TAC

Data	Instructions
Troubleshoot file from the Firepower Management Center (FMC)	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Troubleshoot file from the Firepower device inspecting the traffic	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Full Session Packet Captures	See this article for instructions

Next Steps

If it has been determined that the Active Authentication component is not the cause of the issue, the next step would be to troubleshoot the Intrusion Policy feature.

Click here to proceed to the next article.