F5 Networks, Inc.

Military Unique Deployment Guide

APL STIG / SRG

Version 2.7.2 for TMOS 15.1

August Winterstein – Federal Systems Engineer

MUDG@f5.com

2023-05-01

VERSION HISTORY

DATE	DOCUMENT VERSION	REVISION HISTORY	AUTHOR
11-14-2014	1.0	Initial Release	Michael Coleman, M.Coleman@f5.com
11-14-2014	1.1	Added Appendix B: FIPS	Michael Coleman, m.coleman@f5.com
6-15-2015	1.2	Minor grammar corrections, Syntax Correction: STIG NET1646, STIG NET1647	Michael Coleman, m.coleman@f5.com
6-6-2016	1.3	Added RPM Patch Validation, Encrypted Cookies iRule, HTTPD/SSHD Ciphers, minor grammar corrections.	Michael Coleman, Michael@f5.com
9-29-2016	1.4	Updated to reflect several new values in SRG V1 R2 release. Updated formatting.	Michael Coleman, Michael@f5.com
4-10-2017	1.5	Updated to reflect current ACAS findings (False Positives) and new conditions of fielding. Grammar and spelling corrections.	Michael Coleman, Michael@f5.com
4-14-2017	1.6	Added several new SRG/STIG related items for the new Testing conditions. Added Common Criteria options.	Michael Coleman, Michael@f5.com
5-1-2017	1.7	Updated to reflect configurations implemented during evaluation.	Michael Coleman, Michael@f5.com
7-3-2017	1.8	Updated to reflect mitigations for CAT II findings.	Michael Coleman, Michael@f5.com
7-26-2017	1.9	Updated Conditions of Fielding	Michael Coleman, Michael@f5.com
8-28-2017	2.0	Updated Conditions of Fielding	Michael Coleman, Michael@f5.com
10-6-2017	2.1	Updated Conditions of Fielding	Michael Coleman, Michael@f5.com
12-20-2017	2.2	Added SSL Profile Guidance	Michael Coleman, Michael@f5.com
02-08-2018	2.3	Updated for TIC/APCO CAR finding remediations.	Michael Coleman, Michael@f5.com
03-22-2018	2.4	Updated to reflect current ACAS findings (False Positives).	Anthony Graber, ag@f5.com
05-15-2018	2.5	Updated to reflect current ACAS findings (False Positives).	Anthony Graber, ag@f5.com
11-29-2019	2.6	Updated guidance for 14.1	August Winterstein, MUDG@f5.com
07-19-2021	2.7	Updated guidance for 15.1, added Appendix for ESXi VM config	August Winterstein, MUDG@f5.com
08-09-2021	2.7.1	Updated SSHD “include” steps	August Winterstein, MUDG@f5.com
04-25-2023	2.7.2	Updated guidance for 15.1, added Time Zone configuration, removed references to BIG-IP 11.x STIG IDs	August Winterstein, MUDG@f5.com

DOCUMENT CHANGES, UPDATES & RECOMMENDATIONS

For recommended changes to this document, please contact August Winterstein at MUDG@f5.com

CONTENTS

INTRODUCTION

The following documentation provides guidance on the configuration of BIG-IP in support of APL Deployment.

BASE SOFTWARE REQUIREMENTS

The following base requirements are assumed for this configuration.

- BIG-IP 15.1 or higher

CONDITIONS OF FIELDING

Users must reference and follow the Conditions of Fielding (COF) found in the Cybersecurity Assessment Report (CAR).

STIG / SRG CONFIGURATIONS

The following will detail the configuration items required to configure the BIG-IP appliance to meet the same configurations within the JITC/TIC test facilities.

The following STIGs / SRGs were identified for the Conditions of Fielding requirements and findings related to the Out of Band Management Interface / Control Plane of BIG-IP.

STIGs	Version	Vendor Note
Domain Name System (DNS) SRG	V2R4	Instructions detailed below
Web Server SRG	V3R1	Instructions detailed below
Network Device Management SRG	V4R1	Instructions detailed below
Network Infrastructure Policy STIG	V10R4	Instructions detailed below
Application Layer Gateway (ALG) SRG	V1R2	Instructions detailed below
Intrusion Detection and Prevention Systems (IDPS) SRG	V2R6	Applicable if configured as IDPS
Firewall SRG	V2R3	Applicable if configured as firewall

VMware vSphere Virtual Machine Version 6 STIG	V1R1	Applies to VE running on ESXi only
Virtual Private Network (VPN) SRG	V2R4	Applicable if configured for VPN

LIMIT CONCURRENT GUI SESSIONS

From the BIG-IP GUI:

1. System
2. Preferences
3. Set System Settings view to Advanced
4. Maximum HTTP connections to Configuration Utility

From the BIG-IP Console:

```
tmsh modify sys httpd max-clients <#>

tmsh save sys config
```

REFERENCE: [SRG-APP-000001-NDM-000200] [SRG-NET-000053-ALG-000001]

CONFIGURE TIMEOUTS

HTTPD/TMSH

From the BIG-IP GUI:

1. System
2. Preferences
3. Uncheck “Redirect HTTP to HTTPS”
4. Under Security Settings configure “Idle Time Before Automatic Logout” for 600 seconds or less

From the BIG-IP Console, issue the following commands:

```
tmsh modify sys httpd auth-pam-idle-timeout 600

tmsh modify sys httpd auth-pam-dashboard-timeout on

tmsh modify sys httpd redirect-http-to-https disabled

tmsh modify sys global-settings console-inactivity-timeout 600

tmsh modify cli global-settings idle-timeout 10

tmsh save sys config
```

SSHD

From the BIG-IP GUI:

1. System
2. Configuration
3. Device
4. SSHD
5. Configure "Idle Time Before Automatic Logout" to 600 seconds.

From the BIG-IP Console, issue the following commands:

```
tmsh modify sys sshd inactivity-timeout 600

tmsh save sys config
```

REFERENCE: [SRG-APP-000003-NDM-000202] [SRG-NET-000514-ALG-000514]

LOGON CONSENT BANNER (TMUI)

For all authentication methods (excluding smartcard), from the BIG-IP GUI:

1. System
2. Preferences
3. Security Banner Text To Show On The Login Screen

For all authentication methods (excluding smartcard), from the BIG-IP Console:

```
tmsh modify sys global-settings gui-security-banner enabled

tmsh modify sys global-settings gui-security-banner text 'TEXT'

tmsh save sys config
```

REFERENCE: [SRG-APP-000068-NDM-000215] [SRG-APP-000068-NDM-000216] [SRG-NET-000041-ALG-000022] [SRG-NET-000041-ALG-000023] [SRG-NET-000041-ALG-000024]

LOGON CONSENT BANNER (SSH)

For all authentication methods (excluding smartcard), from the BIG-IP GUI:

1. System
2. Configuration
3. Device
4. SSHD
5. Check the box for “Show The Security Banner On The Login Screen”
6. Enter text in “Security Banner Text To Show On The Login Screen”

For all authentication methods (excluding smartcard), from the BIG-IP Console:

```
tmsh modify sys sshd banner enabled

tmsh modify sys sshd banner-text 'TEXT'

tmsh save sys config
```

Reference: [SRG-APP-000068-NDM-000215] [SRG-APP-000068-NDM-000216] [SRG-NET-000041-ALG-000022] [SRG-NET-000041-ALG-000023] [SRG-NET-000041-ALG-000024]

CONFIGURE TIME ZONE

From the BIG-IP GUI:

1. System
2. Platform
3. Set “Time Zone” to UTC
4. Click Update

From the BIG-IP Console, issue the following commands:

```
tmsh modify sys ntp timezone UTC

tmsh save sys config
```

REFERENCE: [SRG-APP-000374-NDM-000299]

CONFIGURE PRIMARY AND SECONDARY NTP SERVERS

From the BIG-IP GUI:

1. System
2. Configuration
3. Device
4. NTP

From the BIG-IP Console, issue the following commands:

```
tmsh modify /sys ntp servers add {ip_addr ip_addr …}

tmsh save sys config
```

REFERENCE: [SRG-APP-000373-NDM-000298]

NTP AUTHENTICATION

SYMMETRIC KEY AUTHENTICATION

Some of the following procedures involve authenticating NTP packets. Authentication support allows the NTP client to verify that servers are known and trusted, and not intruders intending to masquerade as a legitimate server. This article only describes one authentication method, which is based on symmetric key cryptography; however, you should be aware that other authentication methods are also available.

You must complete this section before implementing any of the configurations described that involve authentication:

***Impact of procedure**: Configuring the NTP with key authentication will require the remaining NTP peers to have the same key.*

1. NTP keys are specified in the **/etc/ntp/keys** file. Each line in this file consists of three fields: the key identifier, the key type, and the passphrase or key itself.
2. Connect to the BIG-IP system command line.
3. Choose a passphrase and define it in the **/etc/ntp/keys** file by executing the following command where **<passphrase>** is the passphrase you have chosen: **`echo "1 M <passphrase> #MD5 Key" > /etc/ntp/keys`**

   For example: `echo "1 M KD6ma870?0AD&uP #MD5 Key" > /etc/ntp/keys` ***Note**: This command assumes that you have not previously configured any other keys in the **/etc/ntp/keys** file. Running this command will overwrite the file.*
4. Restart the **ntpd** service by entering the following command: `tmsh restart /sys service ntpd`
5. Make sure this key is installed on all the NTP servers and clients participating in the NTP time synchronization.
6. Ensure this key will be backup in a UCS archive by adding this key as an entry to the UCS archive entry. You can do so by following the procedure documented in the **Adding a UCS archive entry** section in: https://support.f5.com/csp/article/K4422
7. Optional: You can verify if the NTP authentication is working properly through packet captures by observing that the key IDs are similar for requests as well as responses and the MAC fields are filled.

CONFIGURING THE BIG-IP SYSTEM TO SYNCHRONIZE WITH AN NTP SERVER ONLY IF AUTHENTICATION IS SUCCESSFUL

***Impact of procedure**: None.*

Ensure that you have set up NTP authentication as described in the “Symmetric Key Authentication” section of https://support.f5.com/csp/article/K14120.

Connect to the BIG-IP system command line, issue the following commands:

```
tmsh modify sys ntp include "server [NTP SERVER] key [Trusted Key matched to
/etc/ntp/keys] iburst trustedkey [Trusted Key matched to /etc/ntp/keys]"
```

It may be easier to use edit from tmsh (`edit sys ntp`) and use a text editor to add multiple servers as needed.
Troubleshooting Tip: If you have issues authenticating, verify the strata on the NTP server isn't too high.

Reference: [SRG-APP-000395-NDM-000347]

SNMP COMMUNITY STRINGS

From the BIG-IP GUI:

1. System
2. SNMP
3. Agent
4. Access (v1, v2c)
5. Delete the public community

From the BIG-IP Console, issue the following commands:

```
tmsh modify sys snmp communities delete {"comm-public"}

tmsh save sys config
```

Note: When configuring SNMPv3, the best OID for ALL events is ".1".

REFERENCE: [SRG-APP-000395-NDM-000310]

CONFIGURE LOGGING LEVELS

From the BIG-IP GUI:

1. System
2. Logs
3. Configuration
4. Options
5. Under "Local Traffic Logging":
    a. MCP: Notice
    b. SSL: Informational
    c. Traffic Management OS: Informational
6. Under "Audit Logging":
    a. MCP: Enable

From the BIG-IP Console:

```
tmsh modify sys daemon-log-settings tmm os-log-level informational

tmsh modify sys daemon-log-settings tmm ssl-log-level informational

tmsh modify sys daemon-log-settings mcpd audit enabled

tmsh modify sys daemon-log-settings mcpd log-level notice

tmsh modify sys db log.ssl.level value informational

tmsh save sys config
```

REFERENCE: [SRG-NET-000074-ALG-000043] [SRG-NET-000075-ALG-000044] [SRG-NET-000076-ALG-000045] [SRG-NET-000077-ALG-000046] [SRG-NET-000078-ALG-000047] [SRG-NET-000079-ALG-000048] [SRG-NET-000492-ALG-000027] [SRG-NET-000494-ALG-000029] [SRG-NET-000495-ALG-000030] [SRG-NET-000496-ALG-000031] [SRG-NET-000497-ALG-000032] [SRG-NET-000498-ALG-000033] [SRG-NET-000499-ALG-000034] [SRG-NET-000500-ALG-000035] [SRG-NET-000501-ALG-000036] [SRG-NET-000502-ALG-000037] [SRG-NET-000503-ALG-000038] [SRG-NET-000505-ALG-000039] [SRG-NET-000513-ALG-000026] [SRG-APP-000080-NDM-000220] [SRG-APP-000091-NDM-000223] [SRG-APP-000095-NDM-000225] [SRG-APP-000096-NDM-000226] [SRG-APP-000097-NDM-000227] [SRG-APP-000098-NDM-000228] [SRG-APP-000099-NDM-000229] [SRG-APP-000100-NDM-000230] [SRG-APP-000101-NDM-000231] [SRG-APP-000319-NDM-000283] [SRG-APP-000343-NDM-000289] [SRG-APP-000495-NDM-000318] [SRG-APP-000499-NDM-000319] [SRG-APP-000503-NDM-000320] [SRG-APP-000504-NDM-000321] [SRG-APP-000505-NDM-000322] [SRG-APP-000506-NDM-000323]

CONFIGURE REMOTE LOGGING

From the BIG-IP GUI:

1. System
2. Logs
3. Configuration
4. Remote Logging

From the BIG-IP Console, issue the following commands:

```
tmsh modify sys syslog remote-servers add { <name> { host <ip address> remote-port
<port> } }

tmsh save sys config
```

CONFIGURING THE BIG-IP SYSTEM TO LOG TO THE REMOTE SYSLOG SERVER USING TCP PROTOCOL

From the BIG-IP Console:

```
tmsh modify /sys syslog include "destination remote_server {tcp(\"<remote syslog server IP>\" port (514));};filter f_alllogs {level (debug...emerg);};log {source(local);filter(f_alllogs);destination(remote_server);};"
```

CONFIGURING THE LOCAL IP ADDRESS THAT THE SYSLOG BINDS TO FOR SENDING LOGS TO THE REMOTE SYSLOG SERVER

From the BIG-IP Console:

```
tmsh modify sys syslog remote-servers modify { <name> { local-ip <IP address> } }

tmsh save sys config
```

See https://support.f5.com/csp/article/K13080 for more information.

REFERENCE: [SRG-NET-000088-ALG-000054] [SRG-NET-000334-ALG-000050] [SRG-NET-000511-ALG-000051] [SRG-NET-000335-ALG-000053] [SRG-NET-000385-ALG-000138] [SRG-NET-000392-ALG-000141] [SRG-NET-000392-ALG-000142] [SRG-NET-000392-ALG-000143] [SRG-NET-000392-ALG-000147] [SRG-NET-000392-ALG-000148] [SRG-NET-000392-ALG-000149] [SRG-NET-000249-ALG-000146] [SRG-APP-000360-NDM-000295] [SRG-APP-000515-NDM-000325] [SRG-NET-000333-FW-000014] [SRG-NET-000098-FW-000021] [SRG-NET-000392-FW-000042] [SRG-NET-000249-IDPS-00222] [SRG-NET-000334-IDPS-00191] [SRG-NET-000335-IDPS-00014] [SRG-NET-000385-IDPS-00211] [SRG-NET-000392-IDPS-00214] [SRG-NET-000392-IDPS-00215] [SRG-NET-000392-IDPS-00216] [SRG-NET-000392-IDPS-00217] [SRG-NET-000392-IDPS-00218] [SRG-NET-000392-IDPS-00219] [SRG-NET-000511-IDPS-00012] [SRG-APP-000108-WSR-000166] [SRG-APP-000358-WSR-000163]

CONFIGURE LOCAL PASSWORD POLICY

From the BIG-IP GUI:

1. System
2. Users
3. Authentication

From the BIG-IP Console:

```
tmsh modify auth password-policy lockout-duration 900

tmsh modify auth password-policy max-duration 60

tmsh modify auth password-policy expiration-warning 7

tmsh modify auth password-policy max-login-failures 3

tmsh modify auth password-policy min-duration 1
```

```
tmsh modify auth password-policy minimum-length 15

tmsh modify auth password-policy password-memory 5

tmsh modify auth password-policy policy-enforcement enabled

tmsh modify auth password-policy required-lowercase 1

tmsh modify auth password-policy required-numeric 1

tmsh modify auth password-policy required-special 1

tmsh modify auth password-policy required-uppercase 1

tmsh modify sys db password.difok value 8

tmsh save sys config
```

REFERENCE: [SRG-APP-000065-NDM-000214] [SRG-APP-000164-NDM-000252] [SRG-APP-000166-NDM-000254] [SRG-APP-000167-NDM-000255] [SRG-APP-000168-NDM-000256] [SRG-APP-000169-NDM-000257] [SRG-APP-000170-NDM-000329]

DISABLING NON-CRITICAL SERVICES

From the BIG-IP CLI:

```
tmsh modify sys service <service_name> disable

tmsh save sys config
```

List of available daemons: https://support.f5.com/csp/article/K48615077

Reference: [SRG-APP-000142-NDM-000245] [SRG-NET-000131-ALG-000085] [SRG-NET-000131-FW-000025] [SRG-NET-000131-IDPS-00011] [SRG-NET-000132-VPN-000450]

REMOTE AAA

SPECIFYING REMOTE ADMINISTRATIVE USER LDAP OR ACTIVE DIRECTORY SERVER INFORMATION

Prerequisites:

- Verify that the BIG-IP system user accounts have been created on the remote authentication server.
- Verify that the appropriate user groups, if any, are defined on the remote authentication server.
- If you want to verify the certificate of the authentication server, import one or more SSL certificates.
- The OCSP server must support the Nonce extension

You can configure the BIG-IP system to use an LDAP or Microsoft Windows Active Directory server for authenticating BIG-IP system user accounts, that is, traffic that passes through the management interface (MGMT).

Important: *The values you specify in this procedure for the* ***Role****,* ***Partition Access****, and* ***Terminal Access*** *settings do not apply to group-based authorization. These values represent the default values that the BIG-IP system applies to any user account that is not part of a remote role group.*

1. **System** > **Users** > **Authentication**
2. Click **Change**.
3. From the **User Directory** list, select **Remote – ClientCert LDAP**.
4. Change the **Authentication** drop-down to **Advanced** to see all fields.
5. In the **Host** field, type the IP address of the remote server. The route domain to which this address pertains must be route domain **0**.
6. For the **Port** setting, retain the default port number (**636**) or type a new port number. This number represents the port number that the BIG-IP system uses to access the remote server.
7. In the **Remote Directory Tree** field, type the file location (tree) of the user authentication database on the LDAP or Active Directory server. At minimum, you must specify a domain component (that is, **dc=[value]**).
8. For the **Scope** setting, retain the default value (**Sub**) or select a new value. This setting specifies the level of the remote server database that the BIG-IP system should search for user authentication.
9. For the **Bind** setting, specify a user ID login for the remote server:
    a. In the **DN** field, type the distinguished name for the remote user ID.
    b. In the **Password** field, type the password for the remote user ID.
    c. In the **Confirm** field, re-type the password that you typed in the **Password** field.
10. For the **Check Member Attribute in Group** setting, select **Enabled**.
11. To enable SSL-based authentication, from the **SSL** list select **Enabled** and, if necessary, configure these settings:
    a. From the **SSL CA Certificate** list, select the name of a chain certificate, that is, the third-party CA or self-signed certificate that normally resides on the remote authentication server.
    b. From the **SSL Client Key** list, select the name of the client SSL key. Use this setting only when the remote server requires that the client present a certificate.
    c. From the **SSL Client Certificate** list, select the name of the client SSL certificate. Use this setting only if the remote server requires that the client present a certificate.
12. For **CA Certificate** select a previously imported CA Bundle.
13. For **Login LDAP Attribute** specify **userPrincipalName** (note this is case-sensitive).
14. For **Login Filter** specify **[a-zA-Z0-9]\\w*(\?=@)**

15. For **Client Certificate Name Field** choose **Other Name…** then enter **1.3.6.1.4.1.311.20.2.3** in the **OID** field.
16. Change **OCSP Override** to **On** and set these fields to these values:
    a. **OCSP Responder**: http://<IP>/ocsp
    b. **OCSP Response Max Age**: -1
    c. **OCSP Response Time Skew**: 300
    d. **OCSP Response Timeout**: 300
17. From the **Role** list, select the user role that you want the BIG-IP system to assign by default to all BIG-IP user accounts authenticated on the remote server:
18. From the **Partition Access** list, select the default administrative partition that all remotely-authenticated BIG-IP user accounts can access.
19. From the **Terminal Access** list, select one of the following as the default terminal access for remotely-authenticated user accounts:

OPTION	DESCRIPTION
Disabled	Choose this option when you do not want the remotely-stored user accounts to have terminal access to the BIG-IP system.
tmsh	Choose this option when you want the remotely-stored user accounts to have only **tmsh** access to the BIG-IP system.
Advanced Shell	Choose this option when you want the remotely-stored user accounts to have access to the BIG-IP system using the advanced shell (at the system prompt).

20. Click **Finished**.

REFERENCE: [SRG-APP-000033-NDM-000212] [SRG-APP-000153-NDM-000249] [SRG-APP-000317-NDM-000282] [SRG-APP-000516-NDM-000336] [SRG-APP-000033-WSR-000169]

ENABLE SIGNATURE VERIFICATION FOR UPDATES

From the BIG-IP console:

```
tmsh modify /sys db liveinstall.checksig value "enable"

tmsh save sys config
```

Note: for more information see the following URL: https://support.f5.com/csp/article/K15225

REFERENCE: [SRG-APP-000131-NDM-000243] [SRG-APP-000131-WSR-000051] [SRG-APP-000131-WSR-000073]

CONFIGURE SSH SECURITY SETTINGS

The following accounts for Attempt Count, Protocol, Ciphers, MACs, Key Exchange

Note: Sometimes copy and paste will not work due to CrLf character sets. It may be easier to use the edit command instead of modify from the CLI. This will open a text editor (vi/nano) to allow manual edits to the configuration. Example: "`tmsh edit sys sshd`"

Perform these steps from the BIG-IP Console:

1. Access BIG-IP CLI TMOS prompt:

```
tmsh
```

2. Begin editing the running configuration:

```
load sys config from-terminal merge
```

3. Copy the following, and paste into the terminal window:

```
sys sshd {
include "Protocol 2
MaxAuthTries 3
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
MACs hmac-sha1
KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-
hellman-group14-sha1,diffie-hellman-group-exchange-sha256
LoginGraceTime 60
MaxStartups 5"
}
```

4. Press <Enter> to get to a new line
5. Press **CTRL-D** to submit
6. Save the updated running configuration to disk:

```
save sys config
```

Note: For more information on configuring SSHD, please see the following URLs.
https://support.f5.com/csp/article/K80425458 https://support.f5.com/csp/article/K25523031

REFERENCE: [SRG-APP-000411-NDM-000330] [SRG-APP-000412-NDM-000331]

HTTPD CIPHER CONFIGURATION

These commands will disable insecure SSL/TLS versions and weak ciphers for the BIG-IP Configuration Utility.

Note: Depending on the version of TMOS, some ciphers have been removed in DEFAULT, so the cipher strings could be shortened extensively. Please check release notes.

From the BIG-IP Console, issue the following commands:

```
tmsh modify sys httpd ssl-ciphersuite 'FIPS:!RSA:!SSLv3:!TLSv1:!3DES:!ADH'

tmsh modify sys httpd ssl-protocol TLSv1.2

tmsh save sys config
```

Note: For more details on restricting ciphers and protocols for access to the management interface, please see the following URL: https://support.f5.com/csp/article/K02321234

CONFIGURE SERVICES TO USE TLSV1.2

From the BIG-IP console:

```
tmsh modify sys db big3d.minimum.tls.version value TLSV1.2

tmsh modify gtm global-settings general { iquery-minimum-tls-version TLSv1.2 }
```

Note: the second command to modify GTM will only succeed if the DNS module is provisioned on the BIG-IP

REFERENCE: [SRG-NET-000230-ALG-000113] [SRG-APP-000014-WSR-000006] [SRG-APP-000015-WSR-000014] [SRG-APP-000439-WSR-000151] [SRG-APP-000439-WSR-000152] [SRG-APP-000439-WSR-000156]

DISABLE ROOT USER

From the BIG-IP Console:

```
tmsh modify sys db systemauth.disablerootlogin value true

tmsh save sys config
```

REFERENCE: [SRG-APP-000148-NDM-000346] [SRG-APP-000133-NDM-000244]

FIREWALL SRG CONFIGURATION

Note: Follow the steps in this section if configuring the BIG-IP as a firewall.

CONFIGURING FIREWALL MODE

If the BIG-IP is being used as a firewall, it should be configured in “Firewall Mode” (Default Deny). In this mode, no traffic is allowed unless firewall rules are configured to allow it.

From the BIG-IP GUI:

1. Security
2. Options
3. Network Firewall
4. Firewall Options
5. “Virtual Server & Self IP Contexts” configured to “Reject” or “Drop”

See https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-network-firewall-policies-and-implementations/afm-firewall-default-traffic-processing.html for more information.

REFERENCE: [SRG-NET-000202-FW-000039]

CONFIGURE SOURCE ADDRESS FILTERING

If the BIG-IP is being used as a firewall, it should be configured to disallow packets containing an illegitimate source address.

From the BIG-IP GUI:

1. Network
2. VLANs
3. VLAN List
4. Enable **Source Check** and disable **Auto Last Hop** on each VLAN.

From the BIG-IP Console:

```
tmsh modify net vlan <VLAN Name> source-checking enabled

tmsh modify net vlan <VLAN Name> auto-lasthop disabled

tmsh save sys config
```

REFERENCE: [SRG-NET-000364-FW-000042]

CONFIGURING A DEFAULT LOGGING PROFILE

Logging Profiles configure what is logged on the BIG-IP locally and/or remotely. The following steps configure logging in the Global Firewall Policy.

From the BIG-IP GUI:

1. Security
2. Event Logs
3. Logging Profiles
4. Edit the **global-network** profile
5. **Network Firewall** tab
6. Select the **Log Publisher** you want to use (local-db-publisher logs locally)
7. Check the **Log Rule Matches** boxes and any other settings you want to enable
8. Click **Update**

From the BIG-IP Console:

```
tmsh modify security log profile global-network network modify { all { filter { log-acl-match-accept enabled log-acl-match-reject enabled log-acl-match-drop enabled } publisher <name> } }
```

See https://support.f5.com/csp/article/K51266926 for more information.

REFERENCE: [SRG-NET-000492-FW-000006] [SRG-NET-000493-FW-000007] [SRG-NET-000074-FW-000009] [SRG-NET-000075-FW-000010] [SRG-NET-000076-FW-000011] [SRG-NET-000077-FW-000012] [SRG-NET-000078-FW-000013] [SRG-NET-000089-FW-000019]

INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS) SRG CONFIGURATION

Note: Follow the steps in this section if configuring the BIG-IP as an IDS/IPS.

CONFIGURING A DEFAULT LOGGING PROFILE

Logging Profiles configure what is logged on the BIG-IP locally and/or remotely. The following steps configure logging in the Global Firewall Policy.

From the BIG-IP GUI:

1. Security
2. Event Logs
3. Logging Profiles
4. Edit the **global-network** profile
5. Check the box to enable **Protocol Inspection**
6. **Protocol Inspection** tab
7. Select the **Log Publisher** you want to use (local-db-publisher logs locally)
8. Click **Update**

REFERENCE: [SRG-NET-000074-IDPS-00059] [SRG-NET-000075-IDPS-00060] [SRG-NET-000076-IDPS-00061] [SRG-NET-000077-IDPS-00062] [SRG-NET-000078-IDPS-00063] [SRG-NET-000089-IDPS-00010] [SRG-NET-000113-IDPS-00013] [SRG-NET-000113-IDPS-00082]

VIRTUAL PRIVATE NETWORK (VPN) SRG CONFIGURATION

Note: Follow the steps in this section if configuring the BIG-IP for VPN.

CONFIGURING A LOGGING PROFILE

Logging Profiles configure what is logged on the BIG-IP locally and/or remotely. The following steps configure logging in an Access Profile used for client access VPN.

From the BIG-IP GUI:

1. Access
2. Overview
3. Event Logs
4. Settings
5. Click the **Create** button
6. Enter a Name
7. Check **Enable Access System Logs**
8. Click **Access System Logs** on the left side
9. Select the **Log Publisher** you want to use (local-db-publisher logs locally)
10. Click **OK**
11. Use this logging profile in the VPN Access Profile

REFERENCE: [SRG-NET-000077-VPN-000280] [SRG-NET-000078-VPN-000290] [SRG-NET-000079-VPN-000300] [SRG-NET-000088-VPN-000310] [SRG-NET-000089-VPN-000330] [SRG-NET-000091-VPN-000350]

APPENDIX A: ESXI VE CONFIGURATION

Note: Follow the steps in this section if the BIG-IP is a Virtual Edition (VE) running on a VMWare ESXi hypervisor.

Perform these configuration changes to the BIG-IP VE Virtual Machine after deploying it to a VMWare ESXi server. These settings can be added manually to the VM Configuration one at a time or by editing the .vmx file directly and adding them. Please see VMWare documentation for editing a Virtual Machine's .vmx file.

1. Right-click the VM and select **Edit Settings**
2. **VM Options** tab
3. Expand **Advanced**
4. Click **Edit Configuration**
5. Use **Add Parameter** to add the following Key/Value pairs to the VM's configuration.

Key	Value
isolation.tools.autoInstall.disable	TRUE
isolation.tools.copy.disable	TRUE
isolation.tools.dnd.disable	TRUE
isolation.tools.setGUIOptions.enable	FALSE
isolation.tools.paste.disable	TRUE
isolation.tools.diskShrink.disable	TRUE
isolation.tools.diskWiper.disable	TRUE
isolation.tools.hgfsServerSet.disable	TRUE
vmci0.unrestricted	FALSE
logging	FALSE
isolation.monitor.control.disable	TRUE
isolation.tools.ghi.autologon.disable	TRUE
isolation.bios.bbs.disable	TRUE
isolation.tools.getCreds.disable	TRUE
isolation.tools.ghi.launchmenu.change	TRUE

isolation.tools.memSchedFakeSampleStats.disable	TRUE
isolation.tools.ghi.protocolhandler.info.disable	TRUE
isolation.ghi.host.shellAction.disable	TRUE
isolation.tools.dispTopoRequest.disable	TRUE
isolation.tools.trashFolderState.disable	TRUE
isolation.tools.ghi.trayicon.disable	TRUE
isolation.tools.unity.disable	TRUE
isolation.tools.unityInterlockOperation.disable	TRUE
isolation.tools.unity.push.update.disable	TRUE
isolation.tools.unity.taskbar.disable	TRUE
isolation.tools.unityActive.disable	TRUE
isolation.tools.unity.windowContents.disable	TRUE
isolation.tools.vmxDnDVersionGet.disable	TRUE
isolation.tools.guestDnDVersionSet.disable	TRUE
isolation.tools.vixMessage.disable	TRUE
RemoteDisplay.maxConnections	1
RemoteDisplay.vnc.enabled	FALSE
log.keepOld	10
log.rotateSize	100000
tools.setinfo.sizeLimit	1048576
isolation.device.connectable.disable	TRUE
isolation.device.edit.disable	TRUE
tools.guestlib.enableHostInfo	FALSE
vmsafe.enable	FALSE

6. Click **OK**
7. Click **Save**

APPENDIX B: ADDITIONAL MITIGATIONS

LOGON ACTIVITY REPORTING

When this DB variable is set to true, users with roles of admin, resource admin, or auditor will be redirected to the login summary page.

From the BIG-IP CLI:

```
tmsh modify sys db ui.users.redirectsuperuserstoauthsummary value true

tmsh save sys config
```

DISABLE CALL HOME

From the BIG-IP GUI:

1. System
2. Software Management

3. Update Check
4. Disable Automatic Update Check and Automatic Phone Home options

From the BIG-IP console:

```
tmsh modify sys software update auto-check disabled

tmsh modify sys software update auto-phonehome disabled

tmsh save sys config
```

RESTRICT ICONTROL / REST ACCESS

The iControl SOAP API is an XML-based messaging system that you can use to configure and manage the BIG-IP system. Depending on your organizational security requirements, one method to secure access to the iControl API is to allow only trusted IP addresses or range of IP addresses.

By default, the BIG-IP system allows any user with the Administrator role to access the iControl SOAP API, regardless of their source IP address. If you are adding an IP address or range of IP addresses for the first time, you should perform the following replacing the current allowed list with a new list procedure.

From the BIG-IP CLI:

```
tmsh modify sys icontrol-soap allow add { <IP address or IP address range>}

tmsh save sys config
```

CLASSIFICATION BANNER

From the BIG-IP GUI:

1. System
2. Preferences
3. Security Settings: Advanced
4. Check “Show Advisory Banner”
5. Advisory Color
6. Advisory Text

From the BIG-IP CLI:

```
tmsh modify sys db ui.advisory.enabled value “true”

tmsh modify sys db ui.advisory.color value “[green/red]”

tmsh modify sys db ui.advisory.text value “//CLASSIFICATION//”

tmsh save sys config
```

SSL PROFILE CIPHER AND PROTOCOL CONFIGURATION

These configurations are applied to the Client and/or Server SSL profiles to ensure compliance and security. Additional guidance on SSL Profiles can be found here: https://support.f5.com/csp/article/K01770517

Note: Client SSL Profiles are what will be presented to the Client or User when connecting through LTM. Server SSL Profiles are what the BIG-IP will use to access the internal server or application.

CLIENT SSL CIPHERS & PROTOCOLS

1. Log in to the Configuration utility.
2. Navigate to Local Traffic > Profiles.
3. From the SSL menu, select Client.
4. Click Create for a new profile or select the name of an existing profile.
5. Type a name for the SSL profile.
6. From the Configuration menu, select Advanced.
7. For Ciphers, click the Custom box.
8. Ensure the Cipher Suites option is selected.
   In the Ciphers box, type the desired cipher string:

   ```
   HIGH:!RSA:!DES:!TLSv1:!SSLv3:!ECDHE-RSA-AES256-CBC-SHA
   ```

9. Complete the remaining profile settings.
10. Click Finished.

To verify and test which ciphers will be used, you can issue the following command via CLI, this will also allow you to test possible cipher configuration strings:

```
tmm –clientciphers ‘CIPHER’
```

```
[root@f51:Active:Standalone] config # tmm --clientciphers 'HIGH:!RSA:!DES:!TLSv1:!SSLv3:!ECDHE-RSA-AES256-CBC-SHA'
    ID  SUITE                  BITS PROT    METHOD  CIPHER    MAC     KEYX
 0: 49200  ECDHE-RSA-AES256-GCM-SHA384     256  TLS1.2  Native  AES-GCM   SHA384  ECDHE_RSA
 1: 49192  ECDHE-RSA-AES256-SHA384         256  TLS1.2  Native  AES       SHA384  ECDHE_RSA
 2: 49202  ECDH-RSA-AES256-GCM-SHA384      256  TLS1.2  Native  AES-GCM   SHA384  ECDH_RSA
 3: 49194  ECDH-RSA-AES256-SHA384         256  TLS1.2  Native  AES       SHA384  ECDH_RSA
 4: 49167  ECDH-RSA-AES256-SHA            256  TLS1.1  Native  AES       SHA     ECDH_RSA
 5: 49167  ECDH-RSA-AES256-SHA            256  TLS1.2  Native  AES       SHA     ECDH_RSA
 6: 49196  ECDHE-ECDSA-AES256-GCM-SHA384  256  TLS1.2  Native  AES-GCM   SHA384  ECDHE_ECDSA
 7: 49162  ECDHE-ECDSA-AES256-SHA         256  TLS1.1  Native  AES       SHA     ECDHE_ECDSA
 8: 49162  ECDHE-ECDSA-AES256-SHA         256  TLS1.2  Native  AES       SHA     ECDHE_ECDSA
 9: 49188  ECDHE-ECDSA-AES256-SHA384      256  TLS1.2  Native  AES       SHA384  ECDHE_ECDSA
10: 49198  ECDH-ECDSA-AES256-GCM-SHA384   256  TLS1.2  Native  AES-GCM   SHA384  ECDH_ECDSA
11: 49157  ECDH-ECDSA-AES256-SHA         256  TLS1.1  Native  AES       SHA     ECDH_ECDSA
12: 49157  ECDH-ECDSA-AES256-SHA         256  TLS1.2  Native  AES       SHA     ECDH_ECDSA
13: 49190  ECDH-ECDSA-AES256-SHA384      256  TLS1.2  Native  AES       SHA384  ECDH_ECDSA
14:   159  DHE-RSA-AES256-GCM-SHA384     256  TLS1.2  Native  AES-GCM   SHA384  EDH/RSA
15:    57  DHE-RSA-AES256-SHA           256  TLS1.1  Native  AES       SHA     EDH/RSA
16:    57  DHE-RSA-AES256-SHA           256  TLS1.2  Native  AES       SHA     EDH/RSA
17:    57  DHE-RSA-AES256-SHA           256  DTLS1   Native  AES       SHA     EDH/RSA
18:   107  DHE-RSA-AES256-SHA256         256  TLS1.2  Native  AES       SHA256  EDH/RSA
```

```
19:  136 DHE-RSA-CAMELLIA256-SHA      256 TLS1.1 Native CAMELLIA SHA   EDH/RSA
20:  136 DHE-RSA-CAMELLIA256-SHA      256 TLS1.2 Native CAMELLIA SHA   EDH/RSA
21:  163 DHE-DSS-AES256-GCM-SHA384     256 TLS1.2 Native AES-GCM  SHA384 DHE/DSS
22:   56 DHE-DSS-AES256-SHA         256 TLS1.1 Native AES    SHA   DHE/DSS
23:   56 DHE-DSS-AES256-SHA         256 TLS1.2 Native AES    SHA   DHE/DSS
24:   56 DHE-DSS-AES256-SHA         256 DTLS1  Native AES    SHA   DHE/DSS
25:  106 DHE-DSS-AES256-SHA256       256 TLS1.2 Native AES    SHA256 DHE/DSS
26:  135 DHE-DSS-CAMELLIA256-SHA      256 TLS1.1 Native CAMELLIA SHA   DHE/DSS
27:  135 DHE-DSS-CAMELLIA256-SHA      256 TLS1.2 Native CAMELLIA SHA   DHE/DSS
28:  167 ADH-AES256-GCM-SHA384        256 TLS1.2 Native AES-GCM  SHA384 ADH
```

SERVER SSL CIPHERS AND PROTOCOLS

Server SSL profiles follow the same procedure as client SSL profiles, but by following the server option. For more details on Server SSL Profile configuration options, you can go here: https://support.f5.com/csp/article/K14806

RPM PATCH VALIDATION

It is possible to identify the change log to verify CVE patch level of RPM's installed on the Management Interface by performing the following.

1. Issue the following command, substituting in the appropriate RPM
   `rpm -q -changelog [RPM] | grep CVE`

APPENDIX C: ACRONYMS

AAA	Authentication, Authorization, and Accounting
ACAS	Assured Compliance Assessment Solution
AD	Active Directory
APCO	Approved Products Certification Office
API	Application Programming Interface
APL	Approved Products List
BIG-IP	F5 BIG-IP Product Line
CA	Certificate Authority
CAC	Common Access Card
CAR	Corrective Action Report
CAT	Categories
CBC	Cipher-Block Chaining
DISA	Defense Information Systems Agency
DoD	Department of Defense
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPD	HTTP Daemon

IP	Internet Protocol
JITC	Joint Interoperability Test Command
LDAP	Lightweight Directory Access Protocol
LTM	Local Traffic Manager
NTP	Network Time Protocol
OpenSSH	Open Berkley Software Distribution Secure Shell
OS	Operating System
PKI	Public Key Infrastructure
REST	Representational State Transfer
RPM	RPM Package Manager
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SRG	Security Requirements Guide
SSH	Secure Shell
SSHD	SSH Daemon
SSL	Secure Sockets Layer
STIG	Security Technical Implementation Guide
SUT	System Under Test
Syslog	System Log
TCP	Transmission Control Protocol
TIC	Trusted Internet Connection
TLS	Transport Layer Security
TMOS	F5 Traffic Management Operating System
TMSH	F5 Traffic Management Shell
TMUI	F5 Traffic Management User Interface
UCS	User Configuration Set
XML	Extensible Markup Language
VE	Virtual Edition
VM	Virtual Machine

APPENDIX D: FIPS 140-2

F5 BIG-IP FIPS Administration Manual

https://techdocs.f5.com/en-us/bigip-14-0-0/f5-platforms-fips-administration.html