Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Certificates

September 3, 2019
Table of Contents
Introduction ........................................................................................................................................... 4
Existing ASA Configuration .................................................................................................................. 4
Verification of VPN Tunnel Status on ASA ......................................................................................... 8
Topology .............................................................................................................................................. 10
Configuration on FTD .......................................................................................................................... 10
  Network Diagram............................................................................................................................ 10
  License Verification on FMC ............................................................................................................. 11
Configuration Procedure on FTD ....................................................................................................... 11
Configuration on FTD Post Deployment ............................................................................................... 22
Introduction

This document describes the procedure to migrate site-to-site IKEv2 VPN tunnels using certificates (rsa-sig) as a method of authentication from the existing Cisco Adaptive Security Appliance (ASA) to Firepower Threat Defense (FTD), managed by Cisco Firepower Management Center (FMC).

Existing ASA Configuration

The following example illustrates a sample ASA configuration.

```
ASA# show running-config
: Saved
:
: Serial Number: JAD202407HS
: Hardware: ASA5516, 8192 MB RAM, CPU Atom C2000 series 2416 MHz, 1 CPU (8 cores)
: ASA Version 9.12(1)
!
hostname ASA
enable password ***** pbkdf2 no mac-address auto

!
interface GigabitEthernet1/1
no nameif
security-level 0
no ip address
!
interface GigabitEthernet1/2
nameif inside
security-level 100
ip address 192.168.2.1 255.255.255.0
```
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Certificates

Existing ASA Configuration

```plaintext

interface GigabitEthernet1/3
nameif outside
security-level 0

ip address 10.197.222.163 255.255.255.0

interface GigabitEthernet1/4 no nameif
security-level 0 no ip address

------------------ Output Omitted ------------------

!

boot system disk0:/asa9-12-1-flbf-k8.SPA ftp mode passive
dns domain-lookup outside
same-security-traffic permit inter-interface same-security-traffic permit intra-interface

------------------ Output Omitted ------------------

object network LOCAL
subnet 192.168.2.0 255.255.255.0

object network REMOTE
subnet 192.168.1.0 255.255.255.0

------------------ Output Omitted ------------------

access-list cryptoacl extended permit ip object LOCAL object REMOTE

pager lines 24
logging enable
```
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Certificates

Existing ASA Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging timestamp</td>
</tr>
<tr>
<td>logging monitor debugging</td>
</tr>
<tr>
<td>logging buffered debugging</td>
</tr>
</tbody>
</table>

```
------------- Output Omitted -------------

```

```

nat (inside, outside) source static LOCAL LOCAL destination static REMOTE REMOTE no-proxy-arp route-lookup

```

```

route outside 0.0.0.0 0.0.0.0 10.106.67.1 1

```

```

service sw-reset-button

```

```
crypto ipsec ikev2 ipsec-proposal AES-256

```

```
protocol esp encryption aes-256

```

```
protocol esp integrity sha-1

```

```
crypto ipsec security-association pmtu-aging infinite

```

```
crypto map CMAP 1 match address cryptoacl

```

```
crypto map CMAP 1 set peer 10.106.52.213

```

```
crypto map CMAP 1 set ikev2 ipsec-proposal AES-256

```

```
crypto map CMAP interface outside

```

```
crypto map CMAP interface outside

```

```
crypto ca trustpoint SSL_Trustpoint

```

```
keypair SSL_Trustpoint

```

```
crl configure

```

```
crypto ca trustpool policy

```

```
crypto ca certificate chain SSL_Trustpoint

```

```
certificate ca 00e54fa390fac4d43e

```

```
30820595 3082037d a0030201 02020900 e54fa390 fac4d43e 300d0609 2a864886 f70d0101 0b050030 61310b30 0e060355 04061302 494e310b 30090603 5504080c 024b4131 0c300a06 03550407 0c034247 4c311030 0e060355 040a0c07 4a756e69

```

```
70657231 0d300b06 0355040b 0c045443 4f4e3116 30140603 5504030c 0d6b616e

```
```
61762e6a 756e6970 6572301e 170d3139 30343033 3093238 35355a17 0d323430
34303830 39323835 355a3061 310b3009 06035504 06130249 4e310b30 09060035
04080c02 4b41310c 300a0603 5504070c 0342474c 3110300e 06035504 0a0c074a
756e6970 6572310d 300b0603 55040b0c 0454434f 4e311630 14060355 04030c0d
6b616e61 762e6a75 6e697065 72308202 22300d06 092a8648 86f70d01 01010500
0382020f 0308020a 0a028202 0100b64b 069ed584 8d7a19c8 e5536e25 1c6072a4
b192c6b6 d27b4d98 2e338ede de60d119 64bc434c 11ab57ca 4c9427be b13de752 78febc9e ceece00 fe0fedcf 0072c21a
32730cfd 73d9040d 824cfdf7 39111d44 d8509087 a8f496a8 0face3d9 18bcde77 f3a22f0f 9ce4f714 fc087ad9 4c2d7ab9
a94e34c6 f5a8b0a7 8b346d7d 31018005 0f410a2e db37a0fe 60664239 97405c86
55d38151 a7197a16 455d1500 5b27a43d e9cecf77 c13dc4cc a9f8e676 6dc09452 7c7f700 9dc6a757 fb039012 01ab73cf
50d1d31d 8ce31fb7 d52fa025 ed6b0436 28e51af7 9e658e6f 9a44aee9 ade9daef 160d8521 f0839ff4 3f72b6b6 70a8193a
1e4d150e 99c577ec eff20000 02d9d201 a0f8e9ff 2726d0dd a57514f5 39fa9a04 4f044d6c 573ad712 8ada5006 abb91bc2
525f5930 2fa1da42 34addff3 8ac018de

-------- Output Omitted --------

231060c5 46d5ea92 858051cb cee44ff9 771a1859 bcd83710 6abb3c7c de9767d2 64d45c4e 537f42c7 cf8af3b d32a0c6f
26234ce9 13474f4c 6db5751a df892b6a
1fe0e99 2102b308 4c8ebcca 84f85f39 f4ca59a4 4e402f4a 3 quit
certificate 01
30b2052d 30820315 02010100 0d06092a 864886f7 0d01010b 05003061 310b3009
06035504 06130249 4e310b30 09060355 04080c02 4b41310c 300a0603 5504070c
0342474c 3110300e 06035504 0a0c074a 756e6970 6572310d 300b0603 55040b0c
0454434f 4e311630 14060355 04030c0d 6b616e61 762e6a75 6e697065 72308202
0d313930 34303930 39333434 305a170d 32313034 30383039 33343430 5a305831
0b309006 03550406 1304944e 310b3009 06035504 080c024b 41310c30 0a060355
04070c03 42474c31 10300e06 0355040a 0c07a75 6e697065 72301030 0b060355
040b0404 54434f4e 310d300b 06035504 030c0469 64f3f130 80222230 0d06092a
864886f7 0d010101 05000382 020f0030 82020a02 82020100 9dca303 ddc384d5
Verification of VPN Tunnel Status on ASA

Use the following command to check the encryption and the hashing algorithms used by the tunnel during Phase 1 negotiation.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Certificates

Verification of VPN Tunnel Status on ASA

```
ASA# show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:1, Status:UP- ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote
Status Role
7851179 10.197.222.163/500 10.106.52.213/500
READY RESPONDER


Life/Active Time: 86400/17 sec Session-id: 1
Status Description: Negotiation done
Local spi: A31D53C12DCA9C4A Remote spi: 9D7FB57881A41D9D Local id: 10.197.222.163
Remote id: 10.106.52.213
Local req mess id: 1 Remote req mess id: 2
Local next mess id: 1 Remote next mess id: 2
Local req queued: 1 Remote req queued: 2
Local window: 1 Remote window: 5 DPD configured for 10 seconds, retry 2
NAT-T is not detected
IKEv2 Fragmentation Configured MTU: 576 bytes, Overhead: 28 bytes,

ESP spi in/out: 0x36cdec5d/0x46a1e5ad AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 256, esp_hmac: SHA96 ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
Parent SA Extended Status: Delete in progress: FALSE
Marked for delete: FALSE
```
The above example output shows site-to-site VPN configuration elements for ASA, which depicts the following topology. The example that is shown assumes that the remote peer is a Router.

Topology

Figure 1 - Topology Diagram with ASA

If Figure 1 is similar to the current configuration in ASA, then follow the Configuration Steps to migrate the configuration to FTD.

Note: Ensure that the required interfaces (Physical/Port-channel/Sub-Interface), Routes, NAT, Access Control Policy (ACP) are migrated properly by the Firepower Migration Tool (FMT).

Configuration on FTD

Network Diagram
License Verification on FMC

Ensure that the FMC is registered with the Smart Licensing Portal. In addition, ensure that Export-Controlled Features are enabled.

Configuration Procedure on FTD

Step 1  Migrate the required certificates or Trustpoint as described in Migrating ASA to Firepower Threat Defense Using Certificates document.

Step 2  Navigate to Devices > VPN > Site To Site.
**Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Certificates**

**Configuration on FTD**

**Figure 4 – Create New Site To Site VPN Connection**

![Create New Site To Site VPN Connection](image)

**Step 3** Click Add VPN > Firepower Threat Defense Device.

**Figure 5 – Type of Site to Site VPN**

![Type of Site to Site VPN](image)

**Step 4** Add the Topology Name, Network Topology (Point to Point), the IKE Version as IKEv2. Click the Plus (+) symbol to add a node for the VPN tunnel.

**Figure 6 – Create New VPN Topology**

![Create New VPN Topology](image)

The configuration that is displayed in Figure 6 uses the following settings:
Step 5  For Node A representing the local endpoint of the VPN tunnel, click the **Plus (+)** symbol to specify the target FTD details and perform the following:

a. Choose **Target FTD as Device**.

b. Choose the Interface on which the VPN will terminate.

c. Select **Local Network** from **Protected Networks**.

**Figure 7 - Add Local Endpoint**

The configuration that is displayed in **Figure 7** uses the following settings:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>FTD-2</td>
</tr>
</tbody>
</table>
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Certificates

Configuration on FTD

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>outside</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.197.222.163</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Bidirectional</td>
</tr>
<tr>
<td>Protected Network</td>
<td>Subnet / IP Address (Network)</td>
</tr>
</tbody>
</table>

If you require more details on the networks that you must communicate over the VPN tunnel, use the **Access List (Extended)** option and define the access-list that will be used for protected networks. This functionality was added from version 6.2.3 of the FMC.

In case the ACL on the ASA makes use of objects you can use the option of Subnet/IP Address. In addition, if the ACL is more detailed, make use of the **Access List (Extended)** option on the FMC.

**Figure 8 – Add Local Protected Network (Using Access List)**

For FMC version 6.2.3 or earlier, use **Protected Networks** to add the **Local and Remote Network Objects** displayed in **Figure 9**.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Certificates
Configuration on FTD

Figure 9 - Add Local Protected Network (FMC version 6.2.3 or earlier)

Step 6 Select Local Network from Protected Networks, and click OK to save the endpoint configuration.

Figure 10 - Add Remote Endpoint (Using Subnet)

Step 7 For Node B representing the remote endpoint of the VPN tunnel, click the Plus (+) symbol to specify the remote peer details, and perform the following:

a. Choose Extranet as Device.

b. Enter the Device Name and WAN IP Address of the remote endpoint.

c. Select Remote Network from Protected Networks.

d. Click OK to save the endpoint configuration.

Note: If the peer device is managed by the same FMC, see Site-to-Site VPN for FTD managed by the same FMC.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Certificates
Configuration on FTD

Figure 11 – Add Remote Endpoint

Note: There is no option to configure the tunnel-group name. The FMC deploys the name of the tunnel-group as the IP address of the peer device.

The configuration that is displayed in Figure 11 uses the following settings:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Extranet</td>
</tr>
<tr>
<td>Device Name</td>
<td>Router</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.106.52.213</td>
</tr>
<tr>
<td>Protected Network</td>
<td>Subnet / IP Address (Network)</td>
</tr>
</tbody>
</table>

Step 8 Create a New IKEv2 Policy to match the VPN Phase 2 settings existing on the ASA.

To find the IKE policy used by the VPN tunnel, see Verification of VPN tunnel on ASA.

a. Navigate to the IKE tab.

b. Click the Plus (+) symbol to add a new IKEv2 Policy.
c. Specify the IKE parameters.

d. Click **Save**.

**Figure 12 - New IKEv2 Policy**

![Image of New IKEv2 Policy](image)

The configuration that is displayed in **Figure 12** uses the following settings:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>IKEv2- AES- 256- SHA</td>
</tr>
<tr>
<td>Integrity Algorithm</td>
<td>SHA</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>AES - 256</td>
</tr>
<tr>
<td>PRF Algorithm</td>
<td>SHA</td>
</tr>
<tr>
<td>Diffie- Hellman- Group</td>
<td>5</td>
</tr>
</tbody>
</table>

**Step 9** Select the **Policy** from the drop-down to be used for the VPN tunnel. Change the **Authentication Type** to **Certificates** and proceed to select the trustpoint against **Certificate** option.
Step 10 Create a New IKEv2 IPsec Proposal to match the VPN Phase 2 settings existing on the ASA (you can also edit the default IPsec Proposal to match the parameters).

To create a new IKEv2 IPsec Proposal, perform the following:

a. Navigate to the **IPsec** tab.

b. Click **Edit** to edit the default IKEv2 IPsec Proposal.

c. Click the **Plus (+)** symbol to add a new IKEv2 IPsec Proposal.

d. Specify the IPsec parameters.

e. Click **Save** to save the configuration.
Figure 14 - Create New IKEv2 IPSec Proposal

The configuration that is displayed in Figure 14 uses the following settings:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>AES-256</td>
</tr>
<tr>
<td>ESP Hash</td>
<td>SHA-1</td>
</tr>
<tr>
<td>ESP Encryption</td>
<td>AES-256</td>
</tr>
</tbody>
</table>

Step 11 Select the **IPsec Transform Set** from the list of the **Available Transform Sets**.

Figure 15 - Select IKEv2 IPSec Proposal

Step 12 Confirm that the selected IKEv2 IPSec Proposal is displayed in the **IKEv2 IPSec Proposals**.
Figure 16 – IPsec Settings

Step 13 Navigate to Advanced > Tunnel > Access Control for VPN Traffic.

The traffic that enters the FTD through a VPN tunnel, is subjected to access list checks by default. To bypass the interface ACL check, select the *sysopt connection permit-vpn* check box. Group-policy and per-user authorization access lists still apply to traffic.

**Note:** By default, this setting is enabled on the ASA and is disabled on the FTD.

To get the *sysopt* settings on the ASA, execute the command on the ASA CLI:

```bash
ASA# show running-config all
sysopt no sysopt traffic detailed-statistics no
sysopt connection timewait
sysopt connection tcpmss 1380 sysopt connection
tcpmss minimum 0 sysopt connection permit-vpn
sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows no sysopt
radius ignore-secret

no sysopt noproxyarp inside no sysopt
noproxyarp outside
```
This **Access Control for VPN traffic** bypasses the check from the WAN to LAN zone. Define access control policy to allow traffic from the LAN to the WAN zone.

**Step 14** Click **Save** to save the VPN tunnel configuration on the FMC.

**Figure 17 - Advanced VPN Tunnel Settings**

![Advanced VPN Tunnel Settings](image)

**Figure 18 - Save VPN Settings**

![Save VPN Settings](image)

**Step 15** Select the device to deploy the changes, and click **Deploy**.
Figure 19 – Deploy Policies

Note: Ensure that the required NAT and Access Control Policy configuration is migrated properly by the Firepower Migration Tool (FMT).

Configuration on FTD Post Deployment

```
firepower# show running-config

: Saved

: Serial Number: JAD20140353
: Hardware: ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
: NGFW Version 6.2.3.12
!
hostname firepower
enable password $sha512$5000$q+ve+AWwZxPmzkSAh+SvTg==$Cizrqb4ziPzWva0kLUr4iw== pbkdf2
names
!
```
interface GigabitEthernet1/2 nameif inside
  cts manual
  propagate sgt preserve- untag policy static sgt disabled trusted
  security- level 100
  ip address 192.168.2.1 255.255.255.0

interface GigabitEthernet1/3 nameif outside
  cts manual
  propagate sgt preserve- untag policy static sgt disabled trusted
  security- level 0
  ip address 10.197.222.163 255.255.254.0

---------- Output Omitted ----------

boot system disk0:/os.img

ftp mode passive
ngips conn- match vlan- id
object network LOCAL
subnet 192.168.2.0 255.255.255.0

object network REMOTE
subnet 192.168.1.0 255.255.255.0
access- list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access- list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access- list CSM_FW_ACL_
advanced permit ipinip any any rule-id 9998
access- list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998 access- list CSM_FW_ACL_ advanced permit gre any any
rule-id 9998
access- list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule- id 9998
access- list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule- id 9998
access- list CSM_FW_ACL_ remark rule-id 268435458: ACCESS POLICY: FTD- 2- ACP -
Mandatory
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Certificates
Configuration on FTD

```plaintext
access-list CSM_FW_ACL_remak rule-id 268435458: L7 RULE: Inside-Outside-VPN-ACP
access-list CSM_FW_ACL advanced permit ip ifc inside object LOCAL ifc outside object REMOTE rule-id 268435458
access-list CSM_FW_ACL remarx rule-id 268435457: ACCESS POLICY: FTD-2-ACP
Default
access-list CSM_FW_ACL remarx rule-id 268435457: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL advanced deny ip any any rule-id 268435457
access-list CSM_IPSEC_ACL_1 extended permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
!
------------ Output Omitted ------------
nat (inside,outside) source static LOCAL LOCAL destination static REMOTE REMOTE no-proxy-arp route-lookup
nat (inside,outside) source dynamic any interface access-group CSM_FW_ACL global
route outside 0.0.0.0 0.0.0.0 10.197.222.1 1

------------ Output Omitted ------------
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
protocol esp encryption aes-256 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite

crypto map CSM_Outside_map 1 match address CSM_IPSEC_ACL_1 crypto map CSM_Outside_map 1 set peer 10.106.52.213
crypto map CSM_Outside_map 1 set ikev2 ipsec-proposal CSM_IP_1 crypto map CSM_Outside_map interface outside
crypto ca trustpoint SSL_Trustpoint 21rollment terminal
crl configure
```
crypto ca certificate chain SSL_Trustpoint

<table>
<thead>
<tr>
<th>certificate</th>
<th>ca 00</th>
</tr>
</thead>
<tbody>
<tr>
<td>30820400</td>
<td>308202e8</td>
</tr>
<tr>
<td></td>
<td>05050030</td>
</tr>
<tr>
<td>63310b30</td>
<td>09060355</td>
</tr>
<tr>
<td></td>
<td>20476f20</td>
</tr>
<tr>
<td>44616464</td>
<td>79204772</td>
</tr>
<tr>
<td></td>
<td>476f2044</td>
</tr>
<tr>
<td>61646479</td>
<td>20436c61</td>
</tr>
<tr>
<td></td>
<td>7574686f</td>
</tr>
<tr>
<td>72697479</td>
<td>301e170d</td>
</tr>
<tr>
<td></td>
<td>39313730</td>
</tr>
<tr>
<td>3632305a</td>
<td>3063310b</td>
</tr>
<tr>
<td></td>
<td>13185468</td>
</tr>
</tbody>
</table>

---------- Output Omitted ----------
e0ad595 629a0dcf 8882c532 0ce42b9f 45e60d9f 289cb1b9 2a5a57ad 3703af1d 7fbb7d9f
quit
crypto ca certificate chain SSL_Trustpoint

certificate ca 1be715

<table>
<thead>
<tr>
<th>certificate</th>
<th>3082047d</th>
<th>30820365</th>
<th>a0030201</th>
<th>0202031b</th>
<th>e715300d</th>
<th>06092a86</th>
<th>4886f70d</th>
<th>01010005</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>00306331</td>
<td>0b300906</td>
<td>03550406</td>
<td>13025553</td>
<td>3121301f</td>
<td>06035504</td>
<td>0a131854</td>
<td>68652047</td>
</tr>
<tr>
<td></td>
<td>6f204461</td>
<td>64647920</td>
<td>47726f75</td>
<td>702c2049</td>
<td>6e632e31</td>
<td>31302f06</td>
<td>0355040b</td>
<td>1328476f</td>
</tr>
<tr>
<td></td>
<td>20446164</td>
<td>64792043</td>
<td>6c617373</td>
<td>20322043</td>
<td>65727469</td>
<td>66696361</td>
<td>74696f6e</td>
<td>20417574</td>
</tr>
</tbody>
</table>

---------- Output Omitted ----------
crypto ikev2 policy 10

authentication rsa-sig

encryption aes-256

integrity sha

group 5
prf sha

lifetime seconds 86400

crypto ikev2 enable outside

crypto ikev1 am disable

--------------- Output Omitted ---------------

tunnel-group 10.106.52.213 type ipsec-l2l tunnel-group 10.106.52.213 general-attributes
default-group-policy .DefaultS2SgroupPolicy tunnel-group 10.106.52.213 ipsec-attributes

ikev2 remote-authentication certificate

ikev2 local-authentication certificate SSL_Trustpoint

! 
group-policy .DefaultS2SgroupPolicy internal group-policy .DefaultS2SgroupPolicy attributes

vpn-idle-timeout 30

vpn-idle-timeout alert-interval 1 vpn-session-timeout none

vpn-session-timeout alert-interval 1 vpn-filter none

vpn-tunnel-protocol ikev2

dynamic-access-policy-record DfltAccessPolicy

!
class-map inspection_default

match default-inspection-traffic

!

--------------- Output Omitted ---------------

Cryptochecksum:b76f6ee4099a9a021b6adb496bee827

: end firepower#