CC Hardening Guide for 12a

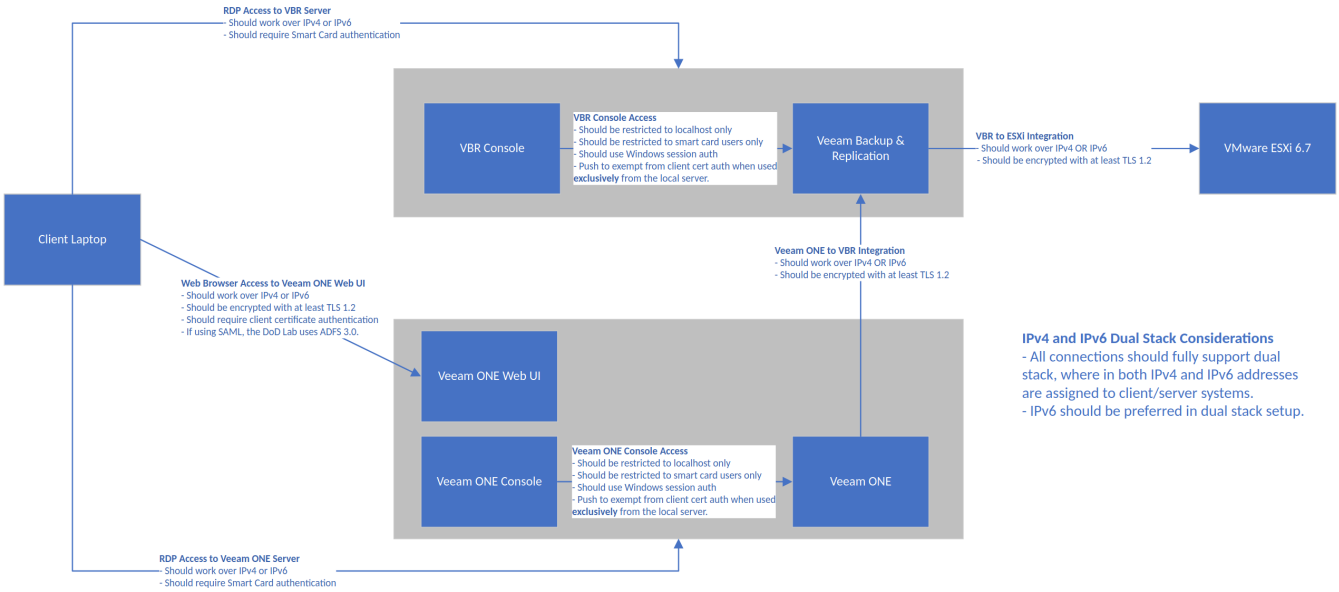
General Security Configuration

Common Criteria Target of Evaluation (TOE) includes the following infrastructure components:

- Veeam Backup and Replication 12a (without Enterprise Manager)
- VeeamOne 12a (without Agent installed on VBR server)
- VMware ESXi 6.7 (without vCenter)

Each Veeam product is installed on a separate server running Windows Server Standard 2019. MS SQL database instance is installed locally, on the same machines with Veeam ONE and VBR.

After installation of Veeam products, you need to configure security settings. Follow the general diagram and specific instructions below.



General comments related to the scheme:

- RDP access is allowed only to the Veeam ONE server and to the backup server. VBR/Veeam ONE Console should be accessible locally.
- The authentication using user/password should be turned off on VBR/Veeam ONE Console.

General Settings for All Windows Servers

Configure the following settings for all Windows servers included in Veeam Backup Infrastructure:

1. Disable LLMNR and NetBIOS broadcast protocols to prevent spoofing and MITM attacks. You can do it in local computer security settings or by group policy.

Disable LLMNR

```
New-Item "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT" -Name DNSClient  -Force
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Name EnableMultiCast -Value 0
-PropertyType DWORD  -Force
```

Disable NetBIOS

```
$regkey = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
Get-ChildItem $regkey |foreach { Set-ItemProperty -Path "$regkey\$($_.pschildname)" -Name NetbiosOptions
-Value 2 -Verbose}
```

2. Disable the obsolete and insecure SMB1 protocol.

Turn off SMB 1

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
```

3. Enable SMB Signing to prevent NTLMv2 relay attacks. Also, enable SMB encryption to ensure that SMB traffic is encrypted.

Turn on SMB Signing and encryption

```
Set-SmbServerConfiguration -RequireSecuritySignature $True -EnableSecuritySignature $True -EncryptData
$True -Confirm:$false
```

4. Enable the FIPS policy to ensure that encryption algorithms are compliant with FIPS 140-2.

FIPS 140

```
Set-ItemProperty -Path Registry::
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\fipsAlgorithmPolicy -Name Enabled -Value "1"
```

5. Disable obsolete TLS 1.0 and TLS 1.1 security protocols.

Disable TLS 1.0

```
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -
Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Server' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Server' -name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client' -
Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Client' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Client' -name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null
Write-Host 'TLS 1.0 has been disabled.'
```

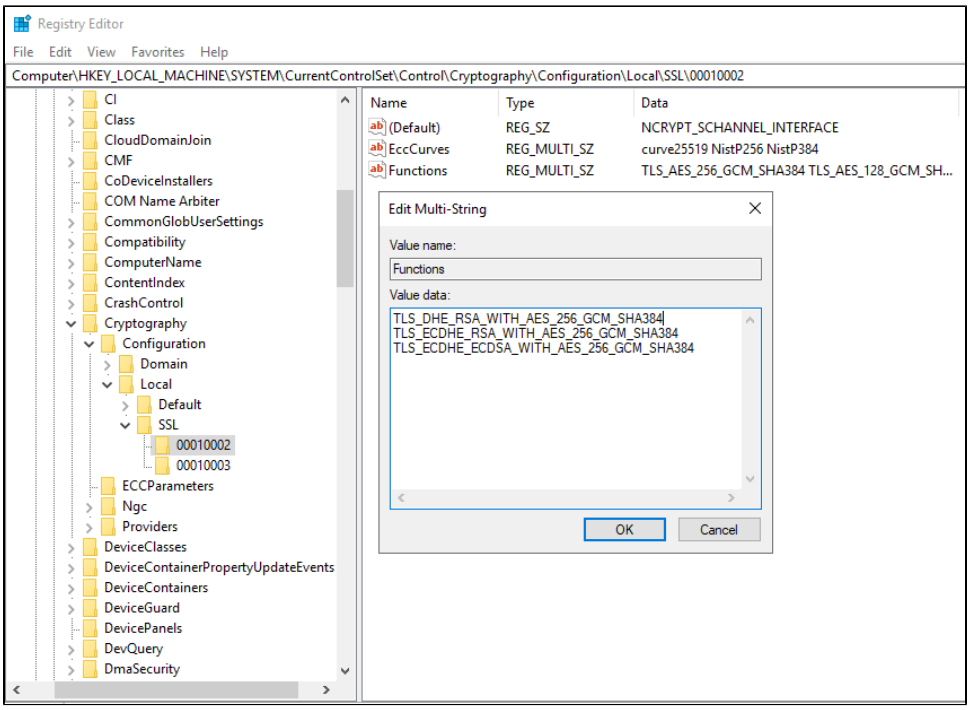
Disable TLS 1.1

```
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -
Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Server' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Server' -name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client' -
Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Client' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Client' -name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null
Write-Host 'TLS 1.1 has been disabled.'
```

6. Disable weak cipher suites and hashing algorithms and check that they are removed from the **Functions** registry entry at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002.

Disable cipher suites

```
Disable-TlsCipherSuite -Name "TLS_AES_256_GCM_SHA384"
Disable-TlsCipherSuite -Name "TLS_AES_128_GCM_SHA256"
Disable-TlsCipherSuite -Name "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA"
Disable-TlsCipherSuite -Name "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA"
Disable-TlsCipherSuite -Name "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA"
Disable-TlsCipherSuite -Name "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA"
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_AES_256_CBC_SHA"
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_AES_128_CBC_SHA"
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_3DES_EDE_CBC_SHA"
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_NULL_SHA256"
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_NULL_SHA"
Disable-TlsCipherSuite -Name "TLS_PSK_WITH_AES_256_GCM_SHA384"
Disable-TlsCipherSuite -Name "TLS_PSK_WITH_AES_128_GCM_SHA256"
Disable-TlsCipherSuite -Name "TLS_PSK_WITH_AES_256_CBC_SHA384"
Disable-TlsCipherSuite -Name "TLS_PSK_WITH_AES_128_CBC_SHA256"
Disable-TlsCipherSuite -Name "TLS_PSK_WITH_NULL_SHA384"
Disable-TlsCipherSuite -Name "TLS_PSK_WITH_NULL_SHA256"
```



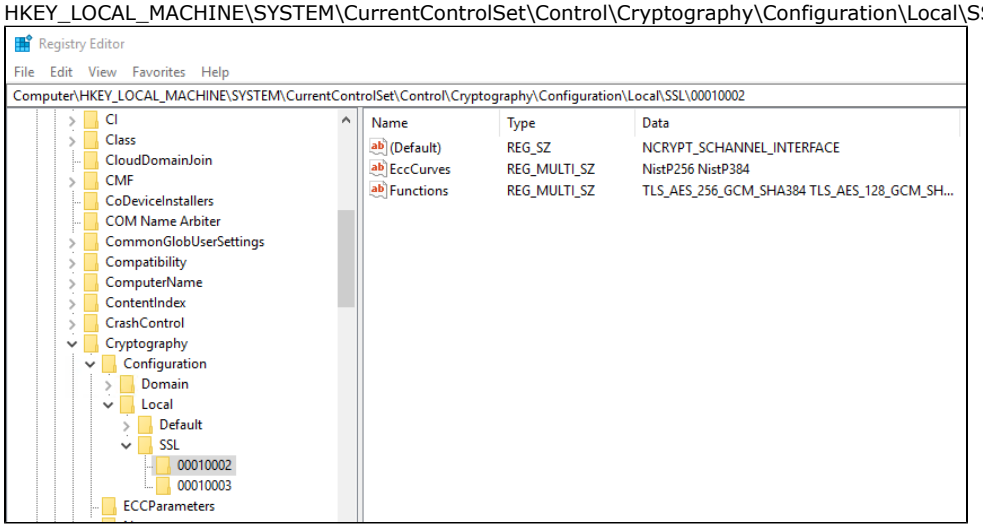
7. Modify the ECC curve priority order to ensure that used elliptic curves are compliant with NIST recommendations:

   a. Disable Curve25519.

   Disable Curve25519

   ```
   Disable-TlsEccCurve -Name curve25519
   ```

   b. Give the ECC curves with `secp*` prefix (NistP256, NistP384) the highest priority. You can do it by using the group policy or changing the **EccCurves** registry entry at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002.

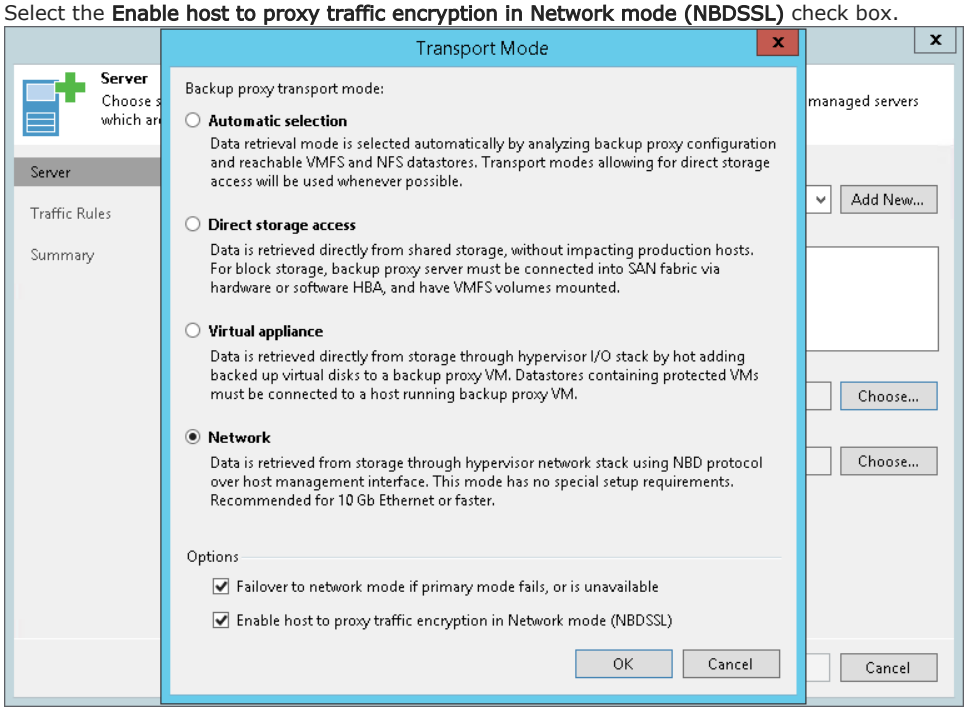


8. Reboot the server to make sure that all settings were applied correctly.

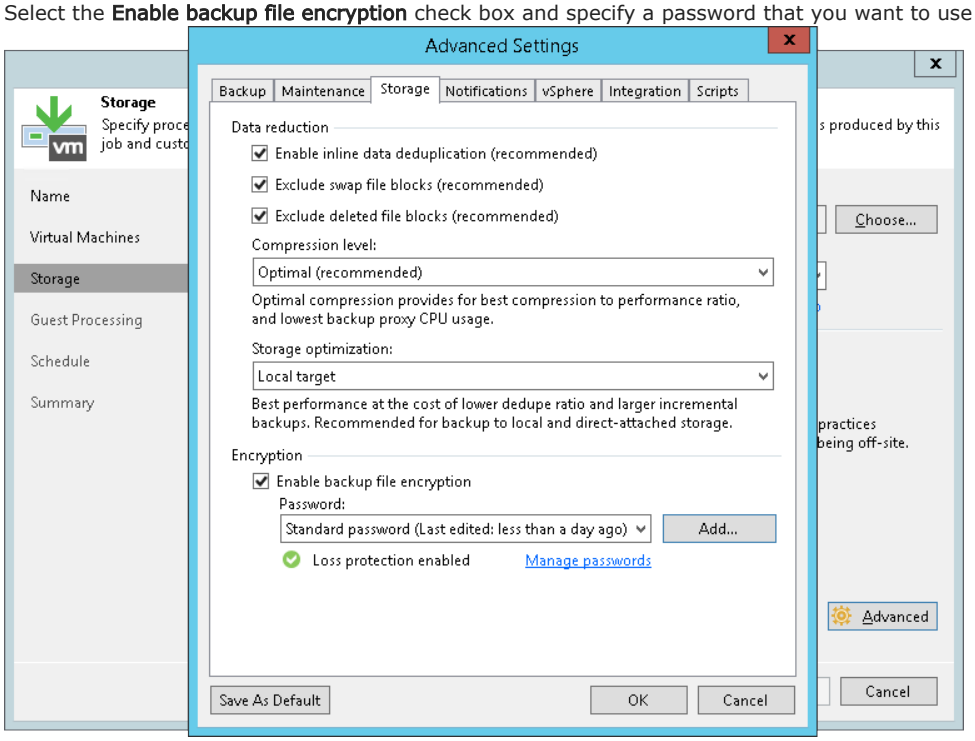
Additional Settings for VBR

1. Configure a TLS certificate to establish a secure connection from backup infrastructure components to the backup server. Follow the instruction to import your TLS certificate signed by a CA. It is recommended for highly secured environments.
2. Enable the FIPS policy on the VBR server to ensure that encryption algorithms are compliant with FIPS 140-2.
3. Enable traffic encryption on the VBR server to encrypt transferred data.

4. If you use the **Network** transport mode for VMware backup proxy, enable proxy traffic encryption to transfer VM data over an encrypted TLS connection:
   a. Open the **Transport Mode** window.
   b. Select the **Enable host to proxy traffic encryption in Network mode (NBDSSL)** check box.



5. Enable backup file encryption to encrypt the content of backup files:
   a. Create a new storage job or edit an existing one.
   b. Go to the **Storage** step of the wizard.
   c. Click **Advanced** and go to the **Storage** tab.
   d. Select the **Enable backup file encryption** check box and specify a password that you want to use for encryption.



6. Create the `C:\ProgramData\VMware\VMware Virtual Disk Development Kit` folder if it doesn't exist. Create the `config.ini` file in the folder and add the following parameters to the file to set up VDDK TLS.

```
tls.protocols=tls1.2
tls.ciphers=ECDHE+AESGCM:RSA+AESGCM
tls.curves=secp384r1:secp521r1
```

7. Reboot the server to make sure that all settings were applied correctly.

Firewall Rules for VBR

Outgoing Connections from the Backup Server			
To	**Protocol**	**Port**	**Description**
ESXi Server	TCP	443	Used for HTTPS connections to ESXi host.
ESXi Server	TCP	902	Used for data transfer to ESXi host.
Incoming Connections to the Backup Server			
From	**Protocol**	**Port**	**Description**
Veeam ONE	TCP	135, dynamically assigned ports	Required to: • Collect data from the backup server through WMI. • Gather CPU and memory performance data from the backup server. Note about dynamically assigned ports: To learn about enabling and disabling WMI traffic, see Connecting to WMI Remotely with VBScript and Setting up a Remote WMI Connection.
Veeam ONE	TCP	445	Required to: • Gather CPU and memory performance data from the backup server. • Access remote registry.
Veeam ONE	TCP	49152 to 65535	Required for Remote Scheduled Tasks Management (RPC). For more information, see this Microsoft KB article.
Management client PC (remote access)	TCP	3389	Used by the Remote Desktop Services.

⚠ All other ports should be closed with the "Deny by default" rule.

Firewall Rules for Veeam ONE

Outgoing Connections from the Veeam ONE			
To	**Protocol**	**Port**	**Description**
Backup Server	TCP	135, dynamically assigned ports	Required to: • Collect data from the backup server through WMI. • Gather CPU and memory performance data from the backup server. **Note about dynamically assigned ports:** To learn about enabling and disabling WMI traffic, see Connecting to WMI Remotely with VBScript and Setting up a Remote WMI Connection.

Backup Server	TCP	445	Required to: • Gather CPU and memory performance data from the backup server. • Access remote registry.
Backup Server	TCP	49152 to 65535	Required for Remote Scheduled Tasks Management (RPC). For more information, see this Microsoft KB article.
Incoming Connections to the Veeam ONE Server			
From	**Protocol**	**Port**	**Description**
Management client PC (remote access)	TCP	3389	Used by the Remote Desktop Services.
Incoming Connections to Veeam ONE Web UI			
From	**Protocol**	**Port**	**Description**
Management client PC	TCP	1239	Used to access Veeam ONE Web UI.

All other ports should be closed with the "Deny by default" rule.