Protection profile of an industrial VPN gateway

Version 1.0 short-term

GTCSI

July 13, 2015

Preface

In the whole document, the acronym ToE (Target of Evaluation) designates the component being evaluated.

Text in red differs from the mid-term version of the protection profile.

1 Product description

1.1 General description

In this protection profile, the ToE is an industrial VPN gateway. It is designed for running in hostile environments where classical VPN gateways could not run properly due to heat, humidity or dust, for instance.

In some cases (Navy, Rail...), certain accreditations are required for the gateway and a classical IT gateway typically does not have such an accreditation.

1.2 Features

The ToE includes the following features:

- **VPN:** The ToE includes features for establishing tunnels with a distant gateway or a road-warrior client. The gateway supports standard protocols (such as IPsec) and implements cryptographical mechanisms which are compliant with ANSSI recommendations.

- **Administration functions:** The ToE includes administration functions in order to configure, or program the other functionalities of the ToE. Several administration interfaces are possible:

    - thick-clients (sometimes also called, depending on the context, administration console, programming workstation...);
    - web-clients;
    - removable devices (USB drives, SD memory cards, etc.).

- **Local logging:** The ToE supports the configuration of a local logging policy. It is possible, in particular, to log security and administration events.

- **Remote logging:** The ToE supports the definition of a remote logging policy. In particular, it is possible to log security and administration events.

1.3   Product usage

From a functional perspective, there are two main use cases for the ToE.

The ToE can establish a tunnel between the network to be protected and a remote network protected by a similar gateway. The two devices ensure the authenticity, the integrity and the confidentiality of the communications between the two networks. This use case is depicted on figure 1.
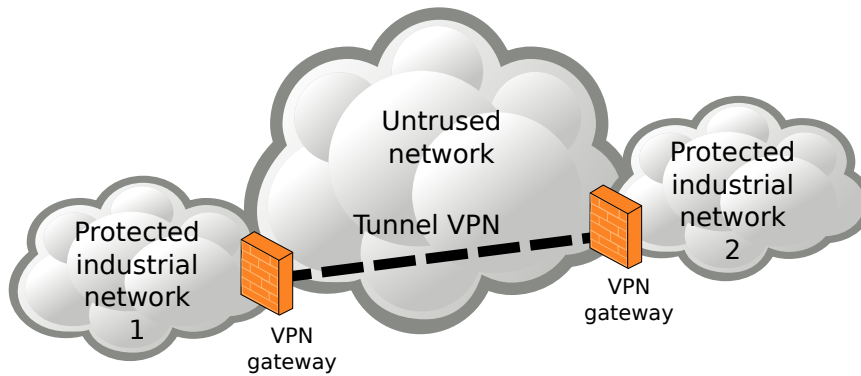
Figure 1: A VPN tunnel between two gateway

The ToE can also establish a tunnel with a road warrior client, that requires access to the protected industrial network. This use case is depicted on figure 2.
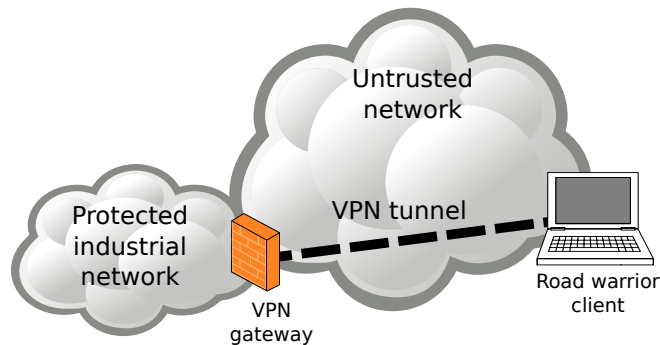
Figure 2: A VPN tunnel with a road warrior client

1.4   Users

The users that may interact with the ToE are the following:

- **Administrator:** user having the permission to modify the configuration of the ToE.

- **Auditor:** User having the permission to consult logs of the ToE.

- **Super-administrator:** User having all the privileges on the ToE. He can, in particular, create, modify or delete user accounts.

- **End-device:** End device directly or indirectly connected to the ToE.

Remark: A user is not necessary a human being, it may be a device or a third-party software. Moreover, the same person may own several user accounts corresponding to different profiles.

1.5 Assumptions

Assumptions on the environment and the use case of the ToE are the following:

- **Logs checking:** We assume that administrators check regularly the local and remote logs produced by the ToE.

- **Administrators:** ToE administrators are competent, trained and trustworthy.

- **Super-administrators:** Super-administrators are trained for performing the tasks they are responsible for. They follow instructions and administration manuals of the ToE and they are not hostile.

- **Premises:** The ToE is located in secure premises with a restricted access limited to trustworthy people. In particular, the attacker does not have access to the physical ports of the ToE.

  Since identical products to the ToE may be purchased freely, the attacker may purchase one in order to research vulnerabilities by any possible mean.

- **Filtering policy:** We assume that the filtering policy configured in the ToE is adapted to the use case.

- **Dimensioning:** We assume the ToE is properly dimensionned for its tasks.

- **Authentication servers:** When appropriate, the authentication servers used for authenticating users are assumed uncompromised and properly configured.

- **Active logging:** We assume that local and remote logging are operational and that local logs are not corrupted.

- **Unevaluated services disabled by default:** Services of the ToE which are not covered by the security target are disabled in the default configuration (also named factory default configuration).

- **Security documentation:** The ToE is provided with a complete documentation for a secure usage. In particular, all secrets are listed in order to allow their customization.

  All recommendations included in this documentation are applied prior to the evaluation.

- **Roadwarrior client:** The roadwarrior client computer is assumed uncompromised and remains so during the evaluation except in case of a failure of the ToE.

2 Critical assets

2.1 Critical assets of the environment

The critical assets of the environment are the following:

- **Encapsulated data flows:** The integrity, authenticity and confidentiality of the data flows in a VPN tunnel must be ensured.

- **Clients authentication:** The ToE ensures the authenticity of the remote device (gateway or roadwarrior client) with which it establishes a tunnel.

- **VPN security policy:** The ToE allows defining a security policy for data flows with roadwarrior clients or a remote gateway. This policy allows

  - defining the list of tunnel peers;
  - defining the list of data flows transiting in each tunnel for each peer;
  - defining the security properties and the cryptographic algorithms used for each tunnel.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Encapsulated data flows		X	X	X
Clients authentication				X
VPN security policy	X		X	
X: mandatory (X): optional				

2.2   ToE critical assets

The critical assets of the ToE are the following:

- **Firmware:** In order to work properly, the firmware must be protected both in integrity and authenticity.

- **Configuration:** The configuration of the ToE must be protected in confidentiality and integrity. The attacker must not be able to discover the configuration of the ToE by other means than the ToE activity.

- **User authentication mechanism:** This mechanism can be based on a local database or on a remote authentication server. In both cases, the ToE must ensure the integrity and authenticity of the mechanism[1].

- **User secrets:** The user secrets can be passwords, certificates… They can be stored in the ToE or stored in a remote authentication server. In all cases, the ToE must ensure the integrity and confidentiality of these credentials.

- **VPN tunnels secrets:** The different credentials used for VPN tunnels must be protected in integrity and confidentiality. They consist in the permanent elements used for establishing a tunnel and the temporary elements such as a session key, used for encrypting and signing data.

- **Access control policy:** The policy can be stored locally or remotely on a authentication server. In both cases, the ToE must ensure the integrity of the access control policy.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Firmware			X	X
Configuration		X	X	
User authentication mechanism			X	X
User secrets		X	X	
VPN tunnels secrets		X	X	
Access control policy			X	
X: mandatory (X): optional				

3   Threat Model

3.1   Attackers

The following attackers are considered:

---

[1]All authentication mechanisms offered by the ToE may not necessarily be part of the security target. However, those which are not included in the security target must be disabled by default.

- **Evil end-device:** A device connected to the ToE is controlled by the attacker.

- **Evil administration device:** A device plugged on the administration network is controlled by the attacker but the attacker may not have valid credentials on the ToE.

3.2 Threats

The following threats are considered:

- **Denial of service:** The attacker manages to generate a denial of service on the ToE by performing an unexpected action or by exploiting a vulnerability (sending a malformed request, using a corrupted configuration file...). This denial of service can affect the whole ToE or only some of its functions.

- **VPN security policy violation:** The attacker manages to bypass the VPN security policy by performing one of the following actions:

    - make unexpected traffic to transit in the tunnel;
    - make some protected traffic to transit outside the tunnel;
    - modify the tunnel characteristics.

- **Firmware alteration:** The attacker manages to inject and run a corrupted firmware on the ToE. The code injection may be temporary or permanent and this does include any unexpected or unauthorized code execution.

    A user may attempt to install that update on the ToE by legitimate means.

    Finally, the attacker manages to modify the version of the firmware installed on the ToE without having the privilege to do so.

- **Configuation alteration:** The attacker manages to modify, temporary or permanently, the ToE configuration.

- **Configuration compromise:** The attacker manages to illegally obtain some parts of the ToE configuration.

- **Credentials theft:** The attacker manages to steal user credentials.

- **Authentication violation:** The attacker succeeds in authenticating himself without credentials.

- **Flows compromise:** In case of data flows requiring confidentiality, the attacker manages to fetch data by intercepting exchanges between the ToE and an external component.

- **Flows alteration:** The attacker manages to corrupt exchanges between the ToE and an external component without being detected.

- **Access control violation:** The attacker manages to obtain permissions that he does not normally have.

4 Security objectives

The following security objectives are considered:

- **Malformed input management:** The ToE has been developed in order to handle correctly malformed input, in particular malformed network traffic.

- **VPN security policy:** The ToE enforces the configured VPN security policy.

- **Secure connection with the authentication server:** The ToE supports secure connection with the authentication server. The secure connection allows authenticating both peers and protecting the integrity and the authenticity of exchanges. It guarantees also non replay of exchanges.

- **Secure storage of secrets:** User secrets are securely stored in the ToE. In particular, the compromise of a file is not sufficient for retrieving them.

- **Secure authentication on administration interface:** Session tokens are protected against hijack and replay. They have a short lifespan. The identity and the permissions of the user account are systematically checked before any privileged action.

- **Access control policy:** The access control policy is strictly applied. In particular, the implementation guarantees the authenticity of privileged operations, i.e. operations that can alter identified critical assets.

- **Firmware signature:** At each update of the firmware, integrity and authenticity of the new firmware are checked before updating.

- **Configuration confidentiality and integrity:** The access control prevents any unauthorized person to read or modify the configuration of the ToE.

A   Critical assets vs threats

	Encapsulated data flows	Clients authentication	VPN security policy	Firmware	Configuration	User authentication mechanism	User secrets	VPN tunnels secrets	Access control policy
Denial of service			Av						
VPN security policy violation			I						
Firmware alteration				I Au					
Configuation alteration					I				
Configuration compromise					C C				
Credentials theft							C I C	C I C	
Authentication violation		Au				I Au			
Flows compromise	C C								
Flows alteration	I Au								
Access control violation									I
Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity									

B   Threats vs security objectives

	Denial of service	VPN security policy violation	Firmware alteration	Configuration alteration	Configuration compromise	Credentials theft	Authentication violation	Flows compromise	Flows alteration	Access control violation
Malformed input management	X									
VPN security policy		X								
Secure connection with the authentication server							X			
Secure storage of secrets						X				
Secure authentication on administration interface				X	X	X	X			
Access control policy										X
Firmware signature			X							
Configuration confidentiality and integrity				X	X			X	X	

C Contributors

This protection profile has been produced by the working group on cybersecurity for industrial systems, supervised by the French Network and Information Security Agency (ANSSI).
The following compagnies and organisms contributed to this document:

- Amossys

- ARC Informatique

- Belden

- DGA/MI

- Gimelec

- Oppida

- Phoenix Contact

- RATP

- Schneider Electric

- Siemens

- Sogeti

- Stormshield

- Thales