

MISE EN PLACE D'UNE CONNEXION SITE A SITE

TECHNICIEN SYSTEME ET RESEAU
MARC VOUA



Table des matières

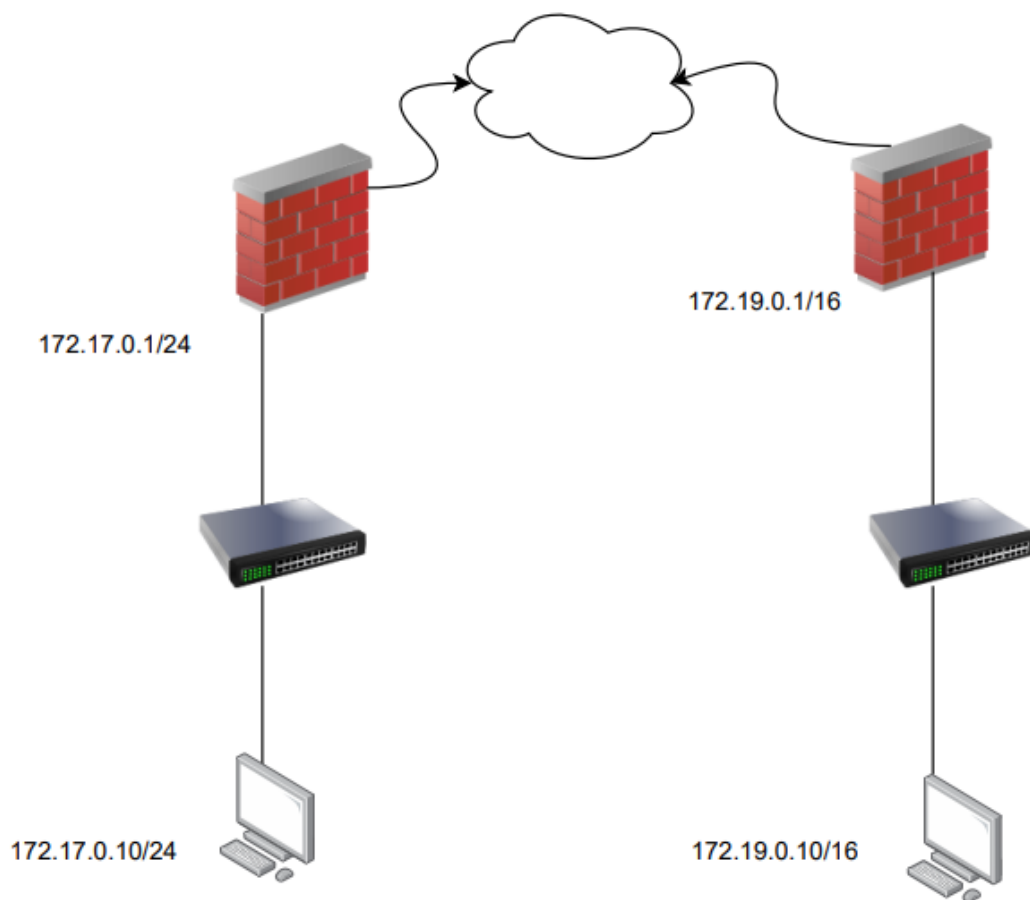
| | | |
|------|--|------------------------------------|
| I- | Cahier des charges – Expression des besoins..... | 2 |
| 1) | Descriptif de l'existant | 2 |
| a) | SCHEMA..... | 2 |
| b) | Tableau d'adressage | Erreur ! Signet non défini. |
| 2) | Besoin | 3 |
| II- | Analyse | 3 |
| 1) | Descriptifs des solutions et choix des solutions | 3 |
| 2) | Prévisions des tests de validation..... | 3 |
| III- | Mise en place | 4 |
| 1) | Schéma, Tableau d'adressage | 4 |
| 2) | Méthodologie | 4 |

I- Cahier des charges – Expression des besoins

1) Descriptif de l'existant

a) SCHEMA

Le client possédant déjà une infrastructure réseau fonctionnelle, il nous présente...



Un schéma avec les différentes adresses IP des machines

2) Besoin

Le service informatique d'une entreprise doit assurer des échanges sécurisés entre plusieurs sites distants, mais aucune connexion fiable et chiffrée n'est en place. Les données circulent parfois via des moyens non sécurisés, ce qui augmente les risques d'interception et de fuite d'informations. Pour améliorer la sécurité des communications et permettre une interconnexion fiable entre les sites, l'entreprise décide de trouver une solution pouvant répondre à ses besoins.

II- Analyse

1) Descriptifs des solutions et choix des solutions

Après une analyse des besoins de l'entreprise et des contraintes liées aux échanges entre sites distants, plusieurs solutions ont été étudiées afin d'améliorer la sécurité et la fiabilité des communications inter-sites. Au regard du manque de chiffrement des échanges, de l'absence de liaison sécurisée entre les différentes infrastructures et de la nécessité de protéger les données transmises, le choix s'est orienté vers la mise en place d'un VPN site à site.

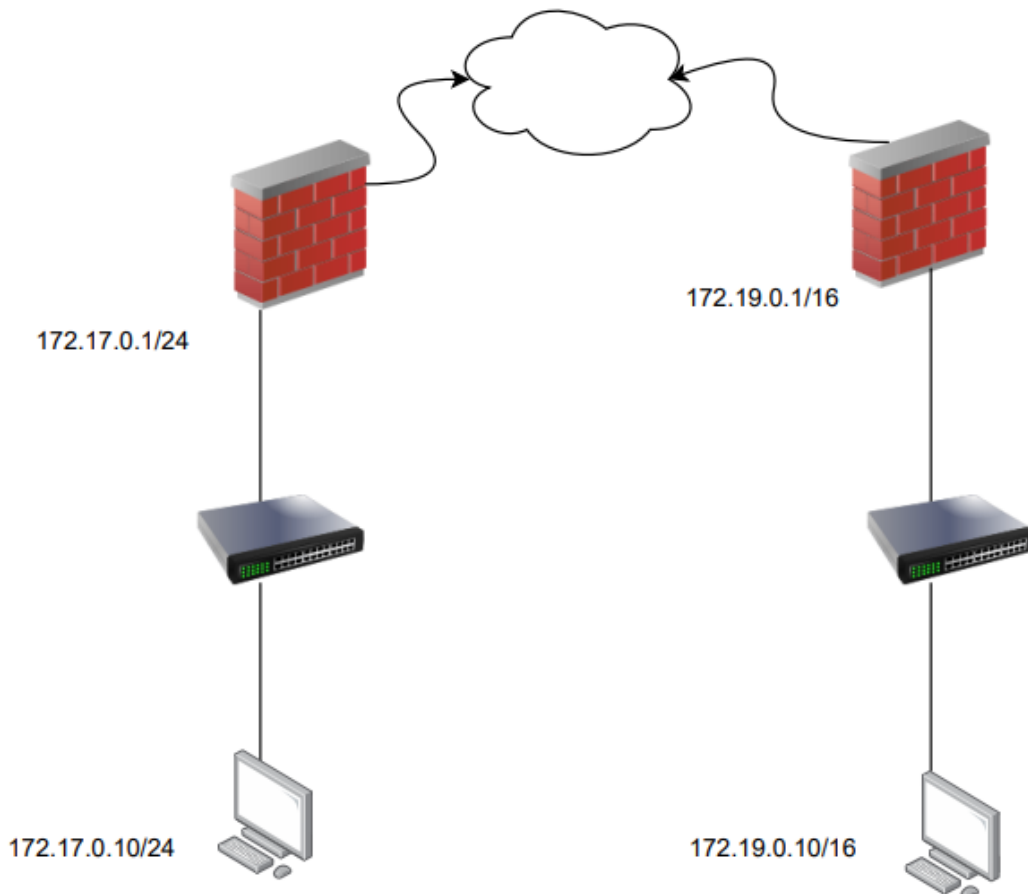
En retenant cette solution, l'entreprise adopte un tunnel sécurisé reliant ses différents sites entre eux via Internet. Le VPN site à site assure le chiffrement des données, l'authentification des équipements et la sécurisation des échanges entre réseaux locaux distants. Ce choix améliore la confidentialité des communications, renforce la sécurité globale du système d'information et constitue une solution fiable, évolutive et adaptée aux besoins d'interconnexion des infrastructures de l'entreprise.

2) Prévisions des tests de validation

Les tests seront réalisés après la mise en place du VPN site à site afin de vérifier le bon fonctionnement du tunnel sécurisé entre les différents sites de l'entreprise. Il consistera à établir des communications entre les réseaux distants afin de s'assurer que les données transitent correctement via le VPN.

III- Mise en place

1) Schéma, Tableau d'adressage



2) Méthodologie

Résultat du ping client 1 avec son parfeu

```
C:\Users\marcvoua>ping 172.17.0.1

Envoi d'une requête 'Ping' 172.17.0.1 avec 32 octets de données :
Réponse de 172.17.0.1 : octets=32 temps<1ms TTL=64
Réponse de 172.17.0.1 : octets=32 temps<1ms TTL=64
Réponse de 172.17.0.1 : octets=32 temps<1ms TTL=64
Réponse de 172.17.0.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.17.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\marcvoua>
```

Résultat du ping client2 avec son parfeu

```
C:\Users\marcvoua>ping 172.19.0.1

Envoi d'une requête 'Ping' 172.19.0.1 avec 32 octets de données :
Réponse de 172.19.0.1 : octets=32 temps<1ms TTL=64
Réponse de 172.19.0.1 : octets=32 temps=10 ms TTL=64
Réponse de 172.19.0.1 :
Statistiques Ping pour 172.19.0.1:
    Paquets : envoyés = 3, reçus = 2, perdus = 1 (perte 33%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 10ms, Moyenne = 5ms
Ctrl+C
^C
```

Configuration phase 1

General Information

Description
A description may be entered here for administrative reference (not parsed).

Disabled Set this option to disable this phase1 without removing it from the list.

IKE Endpoint Configuration

Key Exchange version
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol
Select the Internet Protocol family.

Interface
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway
Enter the public IP address or host name of the remote gateway. [i](#)

Phase 1 Proposal (Authentication)

Authentication Method
Must match the setting chosen on the remote side.

My identifier

Peer identifier

Pre-Shared Key
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.
[Generate new Pre-Shared Key](#)

Phase 1 Proposal (Encryption Algorithm)

| | | | | | |
|-----------------------------|---|---------------------------------------|-------------------------------------|--|------------------------|
| Encryption Algorithm | <input type="text" value="AES256-GCM"/> | <input type="text" value="128 bits"/> | <input type="text" value="SHA256"/> | <input type="text" value="14 (2048 bit)"/> | Delete |
| | Algorithm | Key length | Hash | DH Group | |

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm [+ Add Algorithm](#)

Expiration and Replacement

Life Time
Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

Rekey Time
Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.

Reauth Time
Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.

Rand Time

Configuration phase2

General Information

Description
A description may be entered here for administrative reference (not parsed).

Disabled Disable this phase 2 entry without removing it from the list.

Mode

Phase 1 *No description (IKE ID 1)*

Networks

Local Network /
Type: Address
 Local network component of this IPsec security association.

NAT/BINAT translation /
Type: Address
 If NAT/BINAT is required on this network specify the address to be translated

Remote Network / /
Type: Address

Phase 2 Proposal (SA/Key Exchange)

Protocol
Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

Encryption Algorithms

AES

AES128-GCM

AES192-GCM

AES256-GCM

CHACHA20-POLY1305

Hash Algorithms SHA1 SHA256 SHA384 SHA512 AES-XCBC
Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

PFS key group
Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Keep Alive

Automatically ping host
Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation of a tunnel mode P2, but does not trigger initiation of a VTI mode P2.

Keep Alive Enable periodic keep alive check
Periodically check this P2 and initiate it if disconnected; does not send traffic inside the tunnel. This check ignores the P1 option "Child SA Start Action" and works for both VTI and tunnel mode P2s. For IKEv2 without split connections, this only needs to be enabled on one P2.

[Save](#)

Aperçu de la configuration pour le site A

The changes have been applied successfully.

IPsec Tunnels

| ID | IKE | Remote Gateway | Auth/Mode | P1 Protocol | P1 Transforms | P1 DH-Group | P1 Description | Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------|-----------------------------|-----------------|-----------------------|-------------------|-----------------|----------------|--|----|------|--------------|---------------|-------------|---------------|-----------------|-------------|------------|---|---|---------------|---------------|-----|-------------------|--|---------|--|--|--|--|--|--|--|--|--|--|
| <input type="checkbox"/> Anchor Disable | 1 | V2 WAN 192.168.41.144 | Mutual PSK - | AES256-GCM (128 bits) | SHA256 | 14 (2048 bit) | | Edit Copy Delete | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th>ID</th> <th>Mode</th> <th>Local Subnet</th> <th>Remote Subnet</th> <th>P2 Protocol</th> <th>P2 Transforms</th> <th>P2 Auth Methods</th> <th>Description</th> <th>P2 actions</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Anchor Disable</td> <td>1</td> <td>tunnel LAN</td> <td>172.19.0.0/16</td> <td>ESP</td> <td>AES256-GCM (auto)</td> <td></td> <td>phase 2</td> <td>Edit Copy Delete</td> </tr> <tr> <td colspan="9" style="text-align: center;">+ Add P2</td> </tr> </tbody> </table> | | | | | | | | | ID | Mode | Local Subnet | Remote Subnet | P2 Protocol | P2 Transforms | P2 Auth Methods | Description | P2 actions | <input type="checkbox"/> Anchor Disable | 1 | tunnel LAN | 172.19.0.0/16 | ESP | AES256-GCM (auto) | | phase 2 | Edit Copy Delete | + Add P2 | | | | | | | | |
| ID | Mode | Local Subnet | Remote Subnet | P2 Protocol | P2 Transforms | P2 Auth Methods | Description | P2 actions | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Anchor Disable | 1 | tunnel LAN | 172.19.0.0/16 | ESP | AES256-GCM (auto) | | phase 2 | Edit Copy Delete | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| + Add P2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Configuration phase1 pour le site B

Tunnels Mobile Clients Pre-Shared Keys **Advanced Settings**

General Information

Description
A description may be entered here for administrative reference (not parsed).

Disabled Set this option to disable this phase1 without removing it from the list.

IKE Endpoint Configuration


Key Exchange version
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as

Internet Protocol
Select the Internet Protocol family.

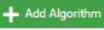
Interface
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway

Phase 1 Proposal (Encryption Algorithm)

| | | | | | |
|-----------------------------|---|---------------------------------------|-------------------------------------|--|---|
| Encryption Algorithm | <input type="text" value="AES256-GCM"/> | <input type="text" value="128 bits"/> | <input type="text" value="SHA256"/> | <input type="text" value="14 (2048 bit)"/> |  |
| | Algorithm | Key length | Hash | DH Group | |

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm 

Expiration and Replacement

Life Time
Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

Rekey Time
Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.

Reauth Time
Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.

Dead Time

Configuration phase2 pour le site B

Tunnels
Mobile Clients
Pre-Shared Keys
Advanced Settings

General Information

Description
A description may be entered here for administrative reference (not parsed).

Disabled Disable this phase 2 entry without removing it from the list.

Mode

Phase 1 phase 1 site B (IKE ID 1)

Networks

Local Network /
Type: Address
Local network component of this IPsec security association.

NAT/BINAT translation /
Type: Address
If NAT/BINAT is required on this network specify the address to be translated

Remote Network / /
Type: Address

Phase 2 Proposal (SA/Key Exchange)

Protocol
Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

Encryption Algorithms

AES

AES128-GCM

AES192-GCM

AES256-GCM

CHACHA20-POLY1305

Hash Algorithms SHA1 SHA256 SHA384 SHA512 AES-XCBC
Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

PFS key group
Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Keep Alive

Automatically ping host
Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation of a tunnel mode P2, but does not trigger initiation of a VTI mode P2.

Keep Alive Enable periodic keep alive check
Periodically check this P2 and initiate it if disconnected; does not send traffic inside the tunnel. This check ignores the P1 option "Child SA Start Action" and works for both VTI and tunnel mode P2s. For IKEv2 without split connections, this only needs to be enabled on one P2.

Save

The changes have been applied successfully.

IPsec Tunnels

| ID | IKE | Remote Gateway | Auth/Mode | P1 Protocol | P1 Transforms | P1 DH-Group | P1 Description | Actions |
|--|-----|-----------------------------|-----------------|-----------------------|-------------------|---------------|----------------|---|
| <input type="checkbox"/> Disable | 1 | V2 WAN 192.168.41.143 | Mutual PSK - | AES256-GCM (128 bits) | SHA256 | 14 (2048 bit) | phase 1 site B | ✎ 📄 🗑️ |
| <input type="checkbox"/> Disable | 1 | tunnel LAN | | ESP | AES256-GCM (auto) | | phase 2 site B | ✎ 📄 🗑️ |

+ Add P2

Le test consiste à ping entre les deux machines des réseau distant

```
C:\Users\marcvoua>ping 172.19.0.10

Envoi d'une requête 'Ping' 172.19.0.10 avec 32 octets de données :
Réponse de 172.19.0.10 : octets=32 temps=1 ms TTL=126
Réponse de 172.19.0.10 : octets=32 temps=1 ms TTL=126
Réponse de 172.19.0.10 : octets=32 temps=1 ms TTL=126
Réponse de 172.19.0.10 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 172.19.0.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\marcvoua>
```

Désactivation du vpn pour le test

| ID | IKE | Remote Gateway | Auth/Mode | P1 Protocol | P1 Transforms | P1 DH-Group | P1 Description | Actions |
|----|-----|-----------------------|------------|-----------------------|---------------|---------------|----------------|---------|
| 1 | V2 | WAN 192.168.41.143 | Mutual PSK | AES256-GCM (128 bits) | SHA256 | 14 (2048 bit) | phase 1 site B | |

Résultat (on constate que le ping ne marche pas)

```
C:\Users\marcvoua>ping 172.17.0.10

Envoi d'une requête 'Ping' 172.17.0.10 avec 32 octets de données :
Délai d'attente de la demande dépassé.
```