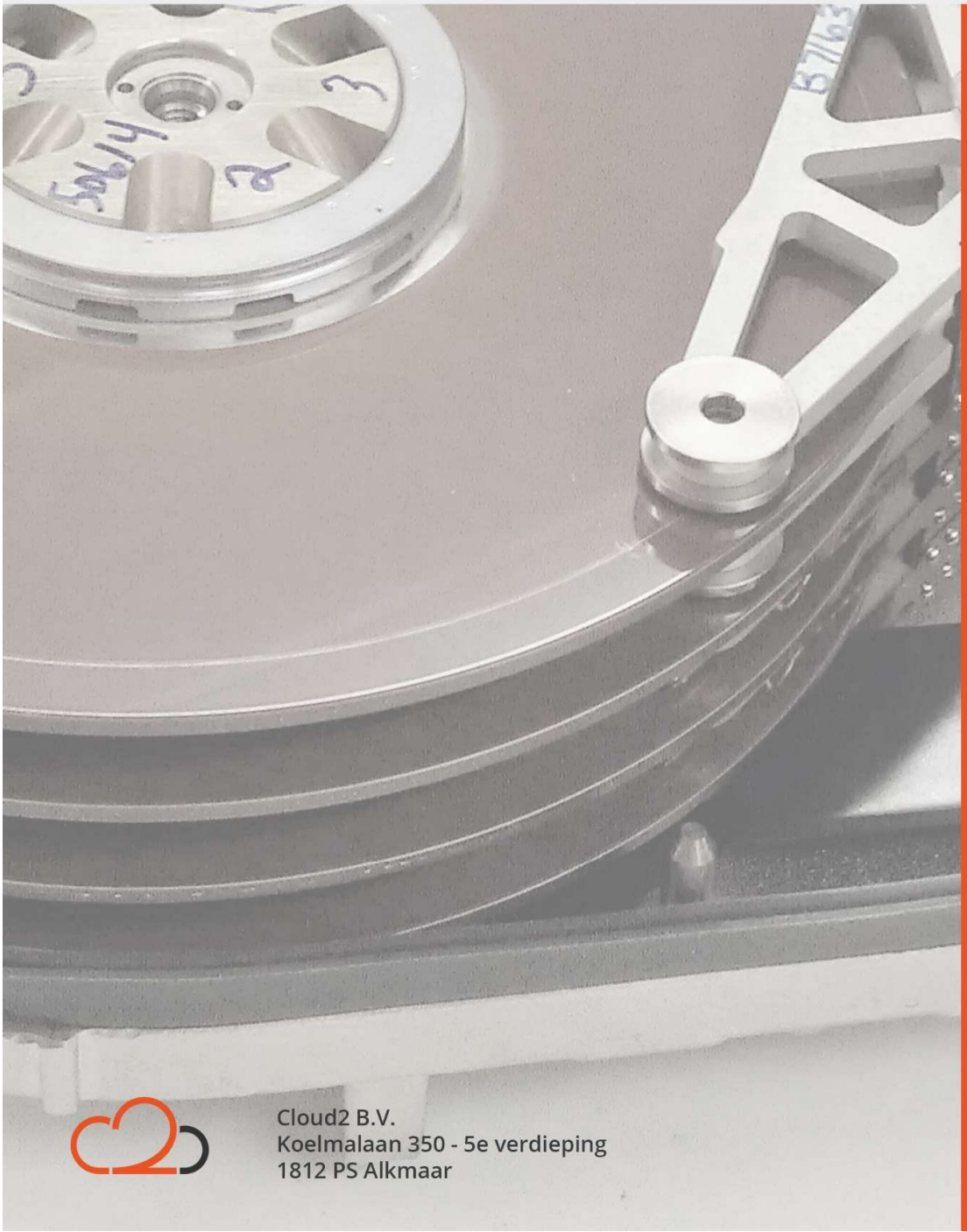
IPSEC SITE-TO-SITE VPN
SOPHOS UTM



Cloud2 B.V.
Koelmalaan 350 - 5e verdieping
1812 PS Alkmaar

Contents

SITE-TO-SITE VPN IN SOPHOS UTM

In deze handleiding wordt beschreven hoe er een site-to-site VPN verbinding opgezet kan worden tussen 2 Sophos UTMs. Het kan handig zijn om een aantal gegevens op papier te zetten betreft de 2 sites die met elkaar verbonden gaan worden.

In deze handleiding hebben wij de onderstaande gegevens als voorbeeld gebruikt:

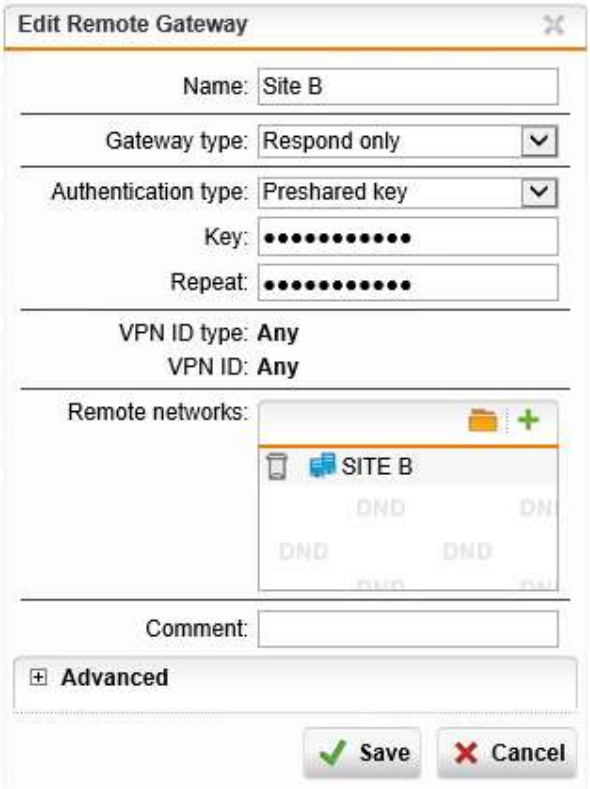
Site A
LAN Intern: 10.0.10.0/24
Public IP: 185.44.x.x

Site B
LAN Intern: 192.168.0.0/24
Public IP: 185.44.x.x

SITE A: MAAK EEN REMOTE GATEWAY AAN

Hiermee wordt een gateway aangemaakt waar Site B naar toe kan verbinden.

1. Login op de WebAdmin van de Sophos UTM.
2. Navigeer naar **Site-to-Site VPN → IPsec → Remote Gateways**.
3. Stel de instellingen als volgt in;



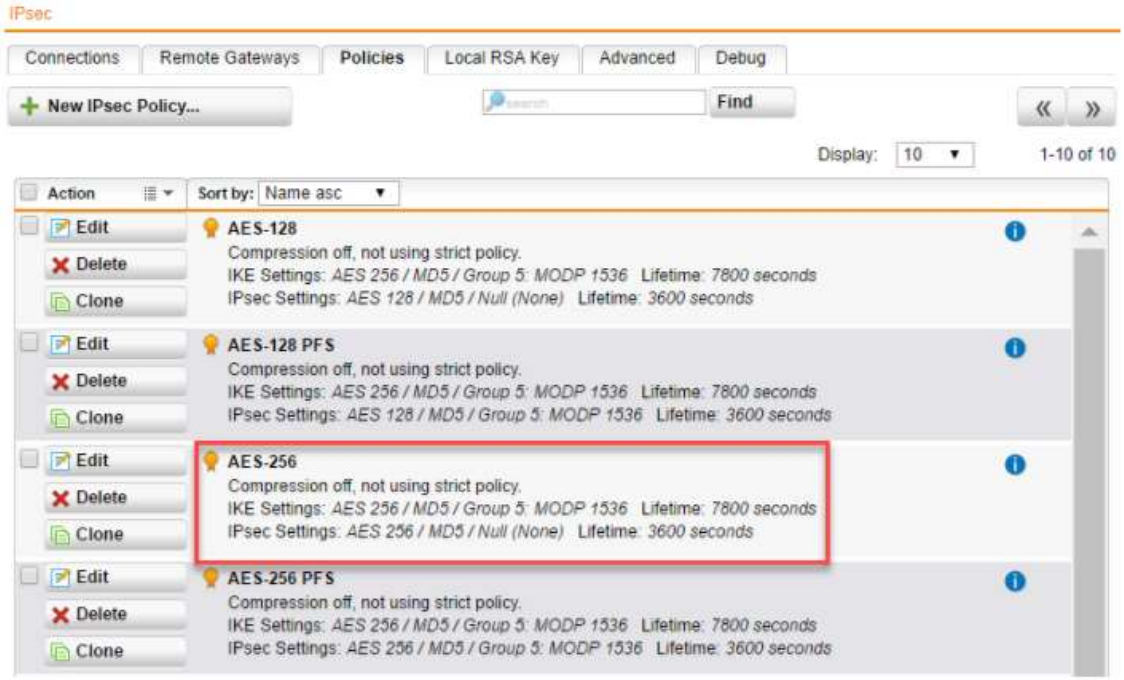
4. Geef een **Naam** op.
5. De Gateway type zou op **Respond Only** gezet moeten worden, Site B gaat namelijk in dit geval de connectie initiëren.

6. Authentication type zetten we op **Preshared key**.
7. Vul de velden Key en Repeat in. Onthoudt deze gegevens, want Site B heeft die ook nodig.
8. Bij **Remote networks** geven we het interne LAN van Site B op wat we willen delen (192.168.0.0/24)
9. Kies voor **Save**.

CONTROLEREN IPSEC POLICY

Met de IPsec Policy wordt de encryptie en andere security parameters ingesteld voor de IPsec tunnel.

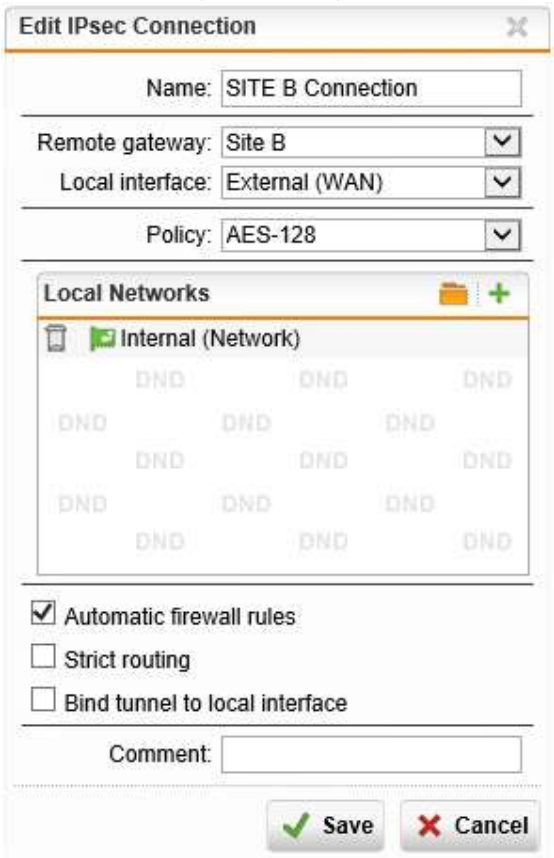
1. Navigeer naar **Site-to-Site VPN → IPsec → Policies**.
2. Beide UTMs moeten dezelfde policy gebruiken.
3. Je kunt op **Edit** klikken naast de policy om te controleren of beide hetzelfde zijn ingesteld.



MAAK EEN IPSEC VERBINDING

Hiermee wordt een IPsec tunnel aangemaakt door het kiezen van een Remote Gateway, een Policy en het defineren van de toegestane lokale netwerken.

1. Navigeer naar **Site-to-Site VPN → IPsec → Connections**.
2. Stel de instellingen als volgt in;

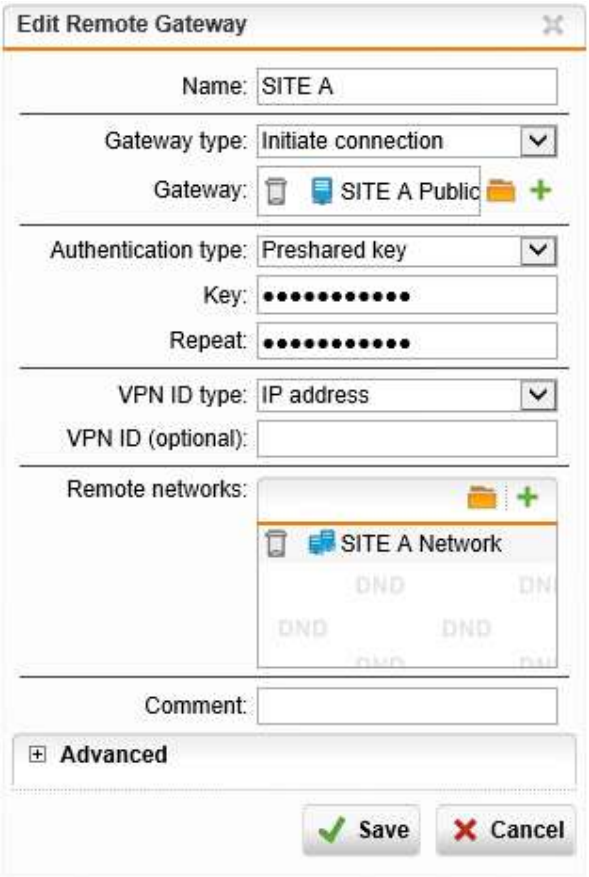


3. Geef een **Name** op voor de tunnel.
4. Selecteer de **Remote gateway** die we eerder hebben aangemaakt.
5. De **Local interface** zou de gateway moeten zijn waarmee de IPsec verbinding wordt opgezet, normaliter de WAN interface.
6. Kies de policy die de omgeving het beste schikt, op beide sites moet deze hetzelfde zijn.
7. Definieer de **Local networks** die toegang krijgen tot de IPsec tunnel (Interne netwerk van Site A).
8. Vink de **Automatic firewall rules** optie aan, anders moeten er handmatig regels aangemaakt worden.
9. Kies voor **Save**.

SITE B: MAAK EEN REMOTE GATEWAY AAN

Hiermee wordt een gateway aangemaakt die connectie initieert naar Site A.

1. Login op de WebAdmin van de Sophos UTM.
2. Navigeer naar **Site-to-Site VPN → IPsec → Remote Gateways**.
3. Stel de instellingen als volgt in;



4. Geef een **Naam** op.
5. De Gateway type zou op **Initiate connection** gezet moeten worden, omdat Site B de connectie gaat opzetten.
6. Bij Gateway maken we een netwerk object aan om het **public IP adres** van Site A op te geven (185.44.x.x).
7. Authentication type zetten we op **Preshared key**.
8. Vul de velden Key en Repeat in. Dit zijn dezelfde gegevens die we hadden opgegeven in Site A.
9. VPN ID type laten we staan op **IP address**.
10. De VPN ID laten we leeg.
11. Bij **Remote networks** geven we het interne LAN van Site A op wat we willen delen (10.0.10.0/24).
12. Kies voor **Save**.

CONTROLEER IPSEC POLICY

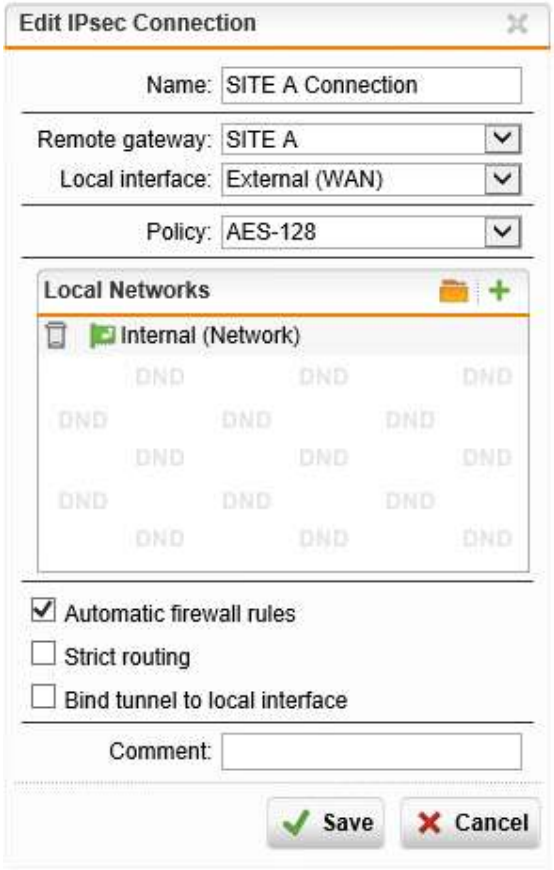
Met de IPsec Policy wordt de encryptie en andere security parameters ingesteld voor de IPsec tunnel.

1. Navigeer naar **Site-to-Site VPN → IPsec → Policies**.
2. Beide UTMs moeten dezelfde policy gebruiken.
3. Je kunt op **Edit** klikken naast de policy om te controleren of beide hetzelfde zijn ingesteld.

MAAK EEN IPSEC VERBINDING

Hiermee wordt een IPsec tunnel aangemaakt door het kiezen van een Remote Gateway, een Policy en het defineren van de toegestane lokale netwerken.

1. Navigeer naar **Site-to-Site VPN → IPsec → Connections**.
2. Stel de instellingen als volgt in;



3. Geef een **Name** op voor de tunnel.
4. Selecteer de **Remote gateway** die we eerder hebben aangemaakt.
5. De **Local interface** zou de gateway moeten zijn waarmee de IPsec verbinding wordt opgezet, normaliter de WAN interface.
6. Kies de policy die de omgeving het beste schikt, op beide sites moet deze hetzelfde zijn.
7. Definieer de **Local networks** die toegang krijgen tot de IPsec tunnel (Interne netwerk van Site B).

8. Vink de **Automatic firewall rules** optie aan, anders moeten er handmatig regels aangemaakt worden.
9. Kies voor **Save**.

CONTROLEER DE VERBINDING

Zodra de verbinding is aangemaakt kun je de status hiervan controleren door te navigeren naar **Site-to-Site VPN**. De kleur van het icoontje aan de linkerkant van de verbinding is **Groen** voor een succesvolle verbinding of **Rood** als er foutmeldingen zijn.

Controleer dit aan beide kanten.

Er zou nu via de CLI een ping check gedaan kunnen worden of de interne LAN-verbindingen elkaar kunnen vinden.

EXTRA INFORMATIE

Zodra de verbinding in de lucht is worden routes automatisch toegevoegd, er hoeft verder niets handmatig gedaan te worden.

Site-to-Site VPN → IPsec → Advanced heeft meerdere tools/objecten die gebruikt kunnen worden om issues te verhelpen. Bijv. de onderstaande:

- **Preshared Key Settings:** hier kan een global public IP adres voor de VPN ID opgegeven worden, of je kan hier de VPN ID type voor alle verbindingen aanpassen.
- **NAT Traversal (NAT-**T): Gebruik NAT traversal om IPsec verkeer door systemen te navigeren die gebruik maken van Network Address Translation (NAT). Ook kun je hier de keepalive interval voor NAT Traversal definiëren. Dit moet op beide sites hetzelfde zijn.