ASDM 6.4: Site-to-Site-VPN-Tunnel mit IKEv2-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie mithilfe von Internet Key Exchange (IKE) Version 2 einen Site-to-Site-VPN-Tunnel zwischen zwei Cisco Adaptive Security Appliances (ASAs) konfigurieren. Es beschreibt die Schritte zur Konfiguration des VPN-Tunnels mithilfe eines ASDM-Assistenten (Adaptive Security Device Manager).

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass die Cisco ASA mit den Grundeinstellungen konfiguriert wurde.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliances der Serie ASA 5500 mit Softwareversion 8.4 und höher
- Cisco ASDM Software Version 6.4 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

IKEv2 ist eine Erweiterung des bestehenden IKEv1-Protokolls, das folgende Vorteile bietet:

- Weniger Nachrichtenaustausch zwischen IKE-Peers
- Unidirektionale Authentifizierungsmethoden
- Integrierte Unterstützung für Dead Peer Detection (DPD) und NAT-Traversal
- Verwendung des Extensible Authentication Protocol (EAP) für die Authentifizierung
- Verhindert das Risiko einfacher DoS-Angriffe durch die Verwendung von Anti-Clogging-Cookies

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

Dieses Dokument zeigt die Konfiguration des Site-to-Site-VPN-Tunnels auf der HQ-ASA. Dasselbe könnte auch als Spiegel auf der BQ-ASA verfolgt werden.

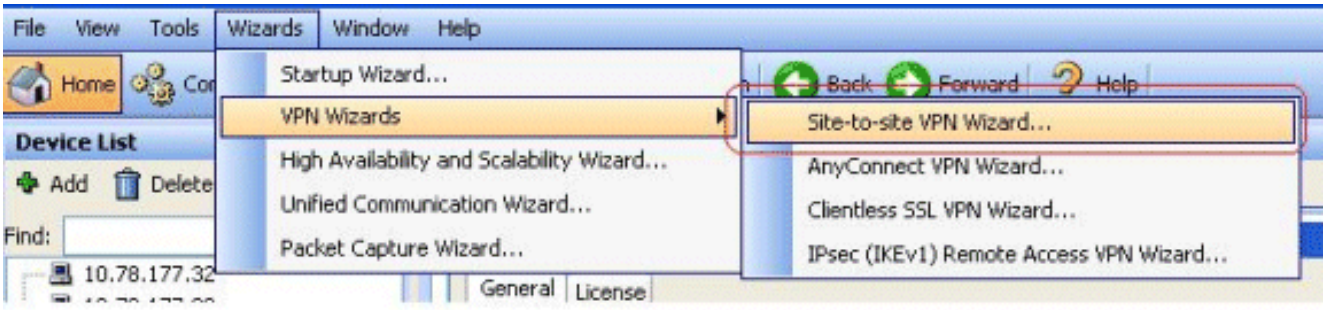
ASDM-Konfiguration auf Hauptsitz-ASA

Dieser VPN-Tunnel kann mithilfe eines benutzerfreundlichen GUI-Assistenten konfiguriert werden.

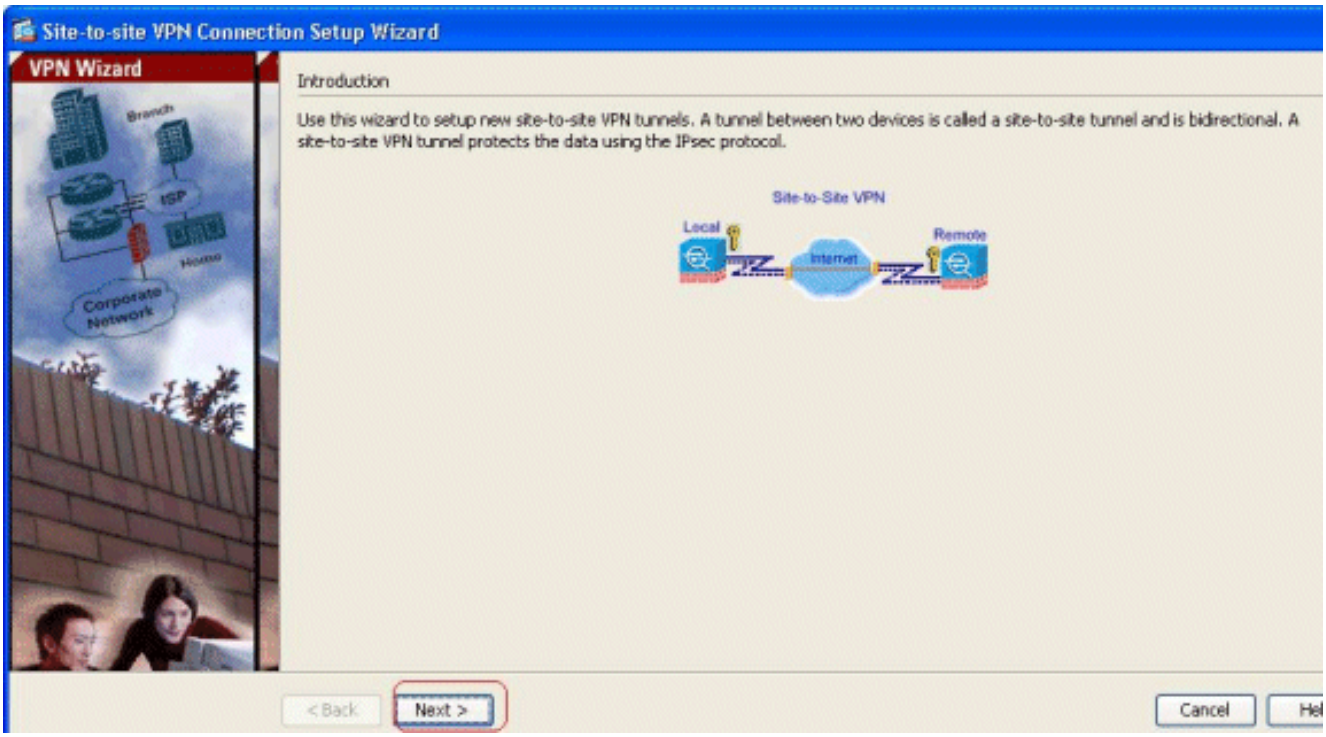
Gehen Sie wie folgt vor:

1. Melden Sie sich beim ASDM an, und gehen Sie zu **Assistenten > VPN-Assistenten > Site-to-**

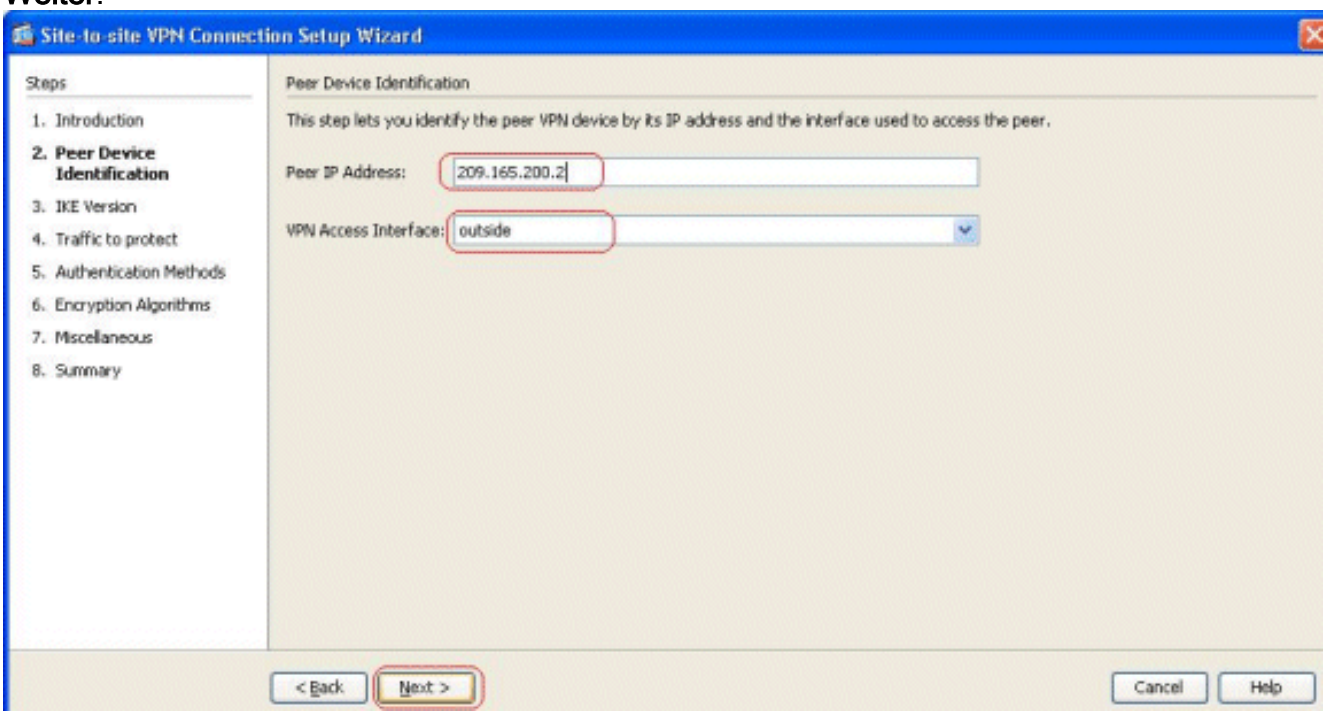
Site-VPN-Assistent.



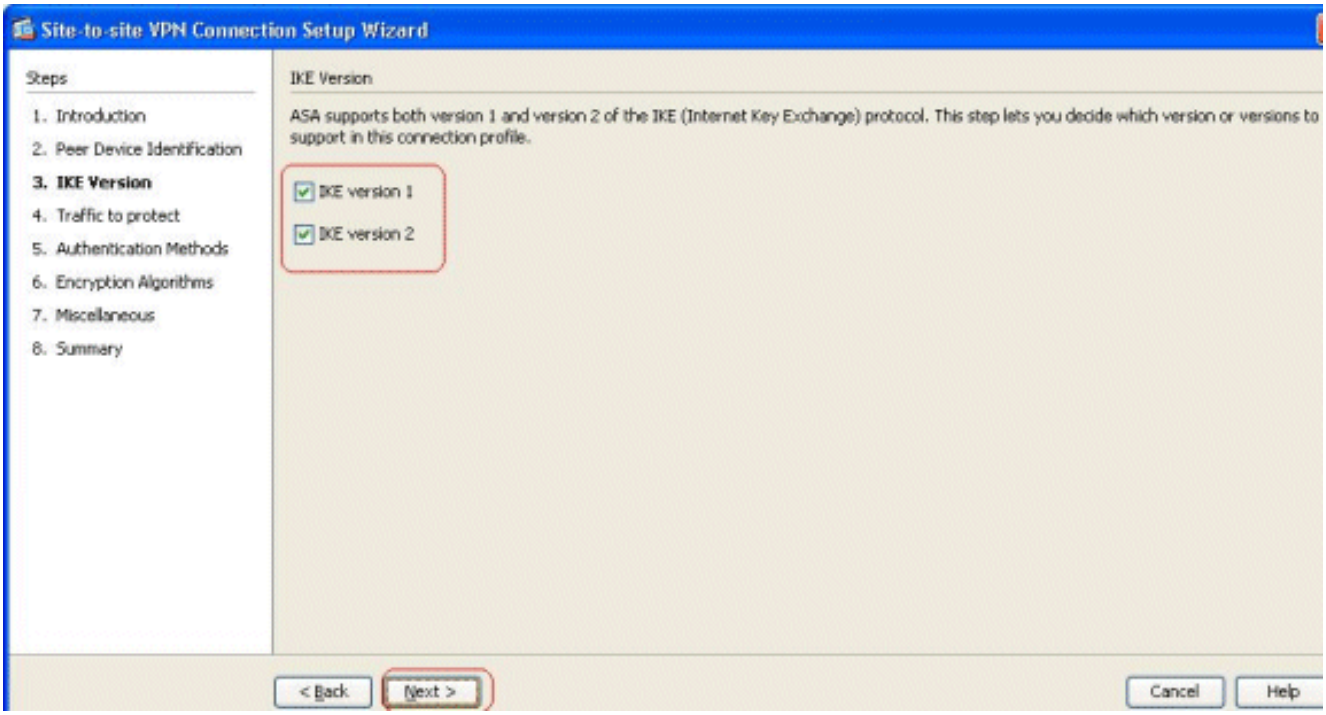
2. Ein Setup-Fenster für eine Site-to-Site-VPN-Verbindung wird angezeigt. Klicken Sie auf **Weiter**.



3. Geben Sie die Peer-IP-Adresse und die VPN-Zugriffsschnittstelle an. Klicken Sie auf **Weiter**.

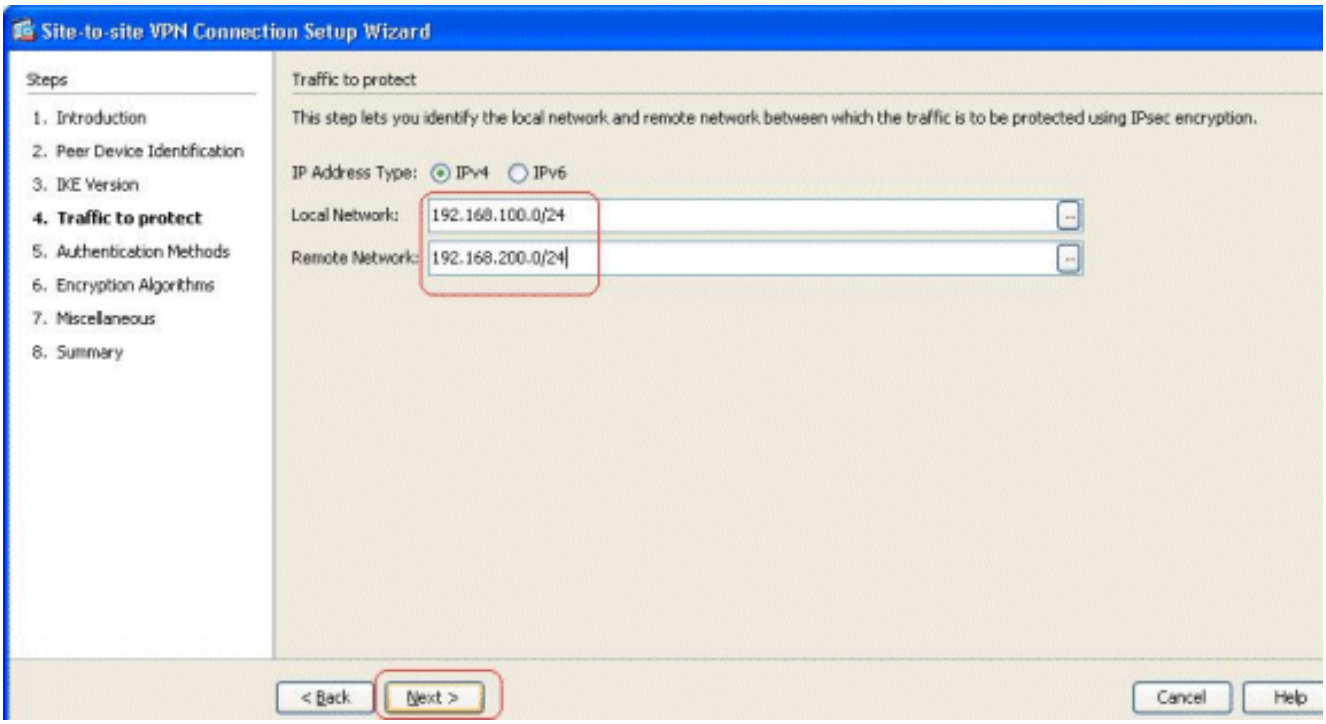


4. Wählen Sie beide IKE-Versionen aus, und klicken Sie auf **Weiter**.

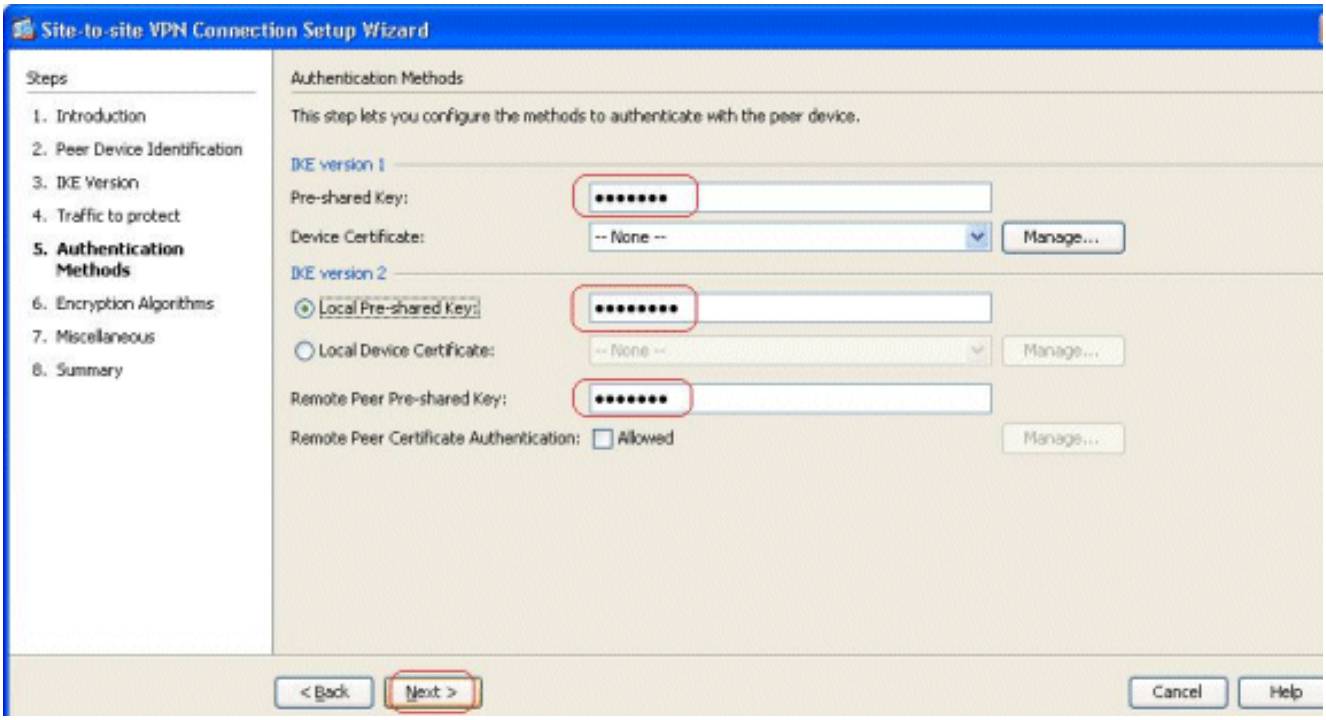


Hinweis: Beide Versionen von IKE sind hier konfiguriert, da der Initiator bei einem Ausfall von IKEv2 eine Sicherung von IKEv2 zu IKEv1 durchführen könnte.

5. Legen Sie das lokale Netzwerk und das Remote-Netzwerk fest, damit der Datenverkehr zwischen diesen Netzwerken verschlüsselt und durch den VPN-Tunnel geleitet wird. Klicken Sie auf **Weiter**.

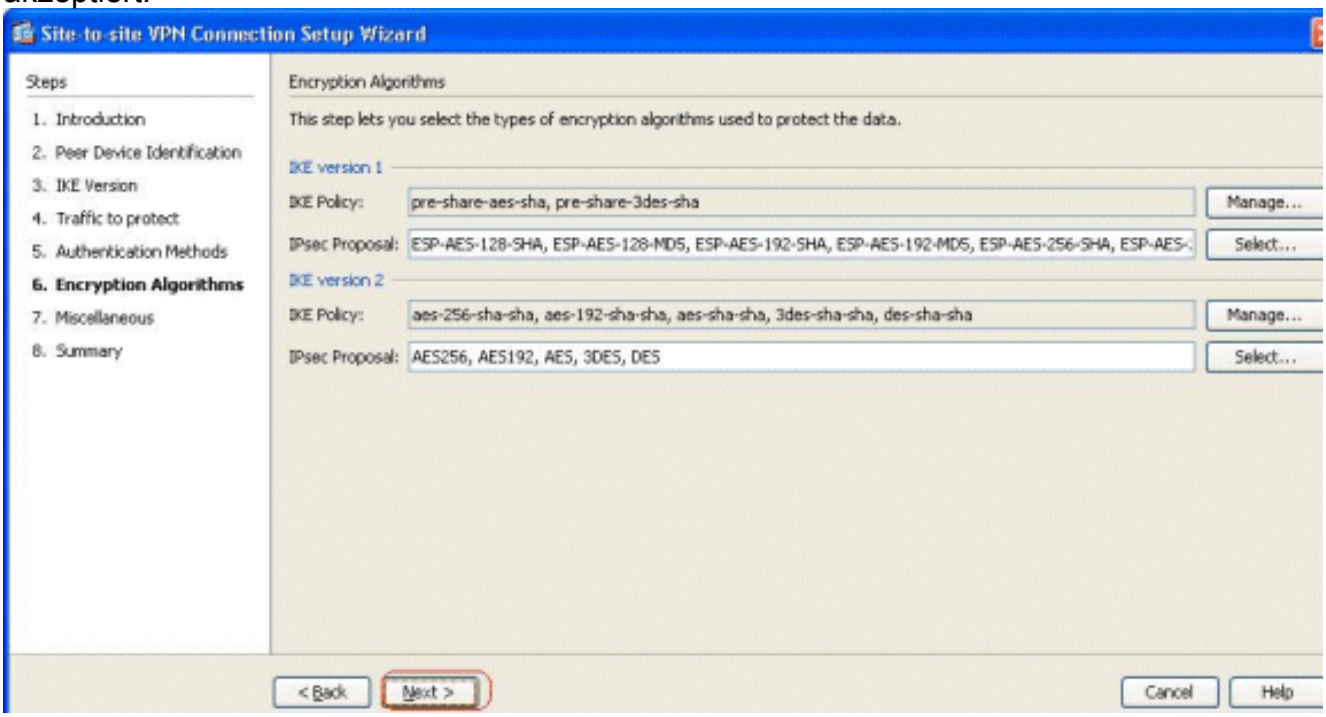


6. Geben Sie die vorinstallierten Schlüssel für beide Versionen von IKE an.

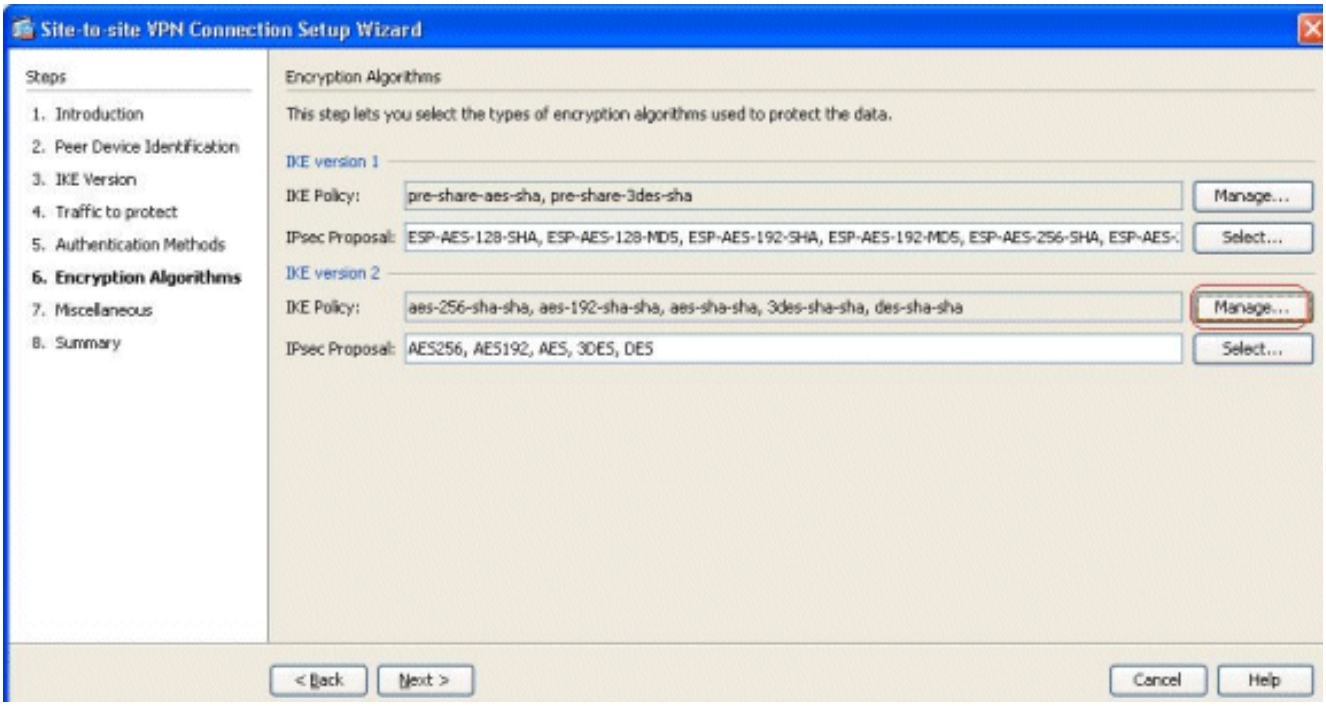


Der Hauptunterschied zwischen IKE-Versionen 1 und 2 besteht in der von ihnen zugelassenen Authentifizierungsmethode. IKEv1 lässt an beiden VPN-Endpunkten nur einen Authentifizierungstyp zu (d. h. einen Pre-Shared Key oder ein Zertifikat). IKEv2 ermöglicht jedoch die Konfiguration asymmetrischer Authentifizierungsmethoden (d. h. Pre-Shared-Key-Authentifizierung für den Ersteller, aber Zertifikatauthentifizierung für den Responder) mithilfe separater lokaler und Remote-Authentifizierungs-CLIs.Darüber hinaus können Sie an beiden Enden verschiedene vorinstallierte Schlüssel verwenden. Der lokale Pre-Shared Key am HQ-ASA-Ende wird zum Remote Pre-Shared Key am BQ-ASA-Ende. Ebenso wird der Remote Pre-Shared Key am HQ-ASA-Ende zum lokalen Pre-Shared Key am BQ-ASA-Ende.

7. Geben Sie die Verschlüsselungsalgorithmen für IKE-Versionen 1 und 2 an. Hier werden die Standardwerte
akzeptiert:

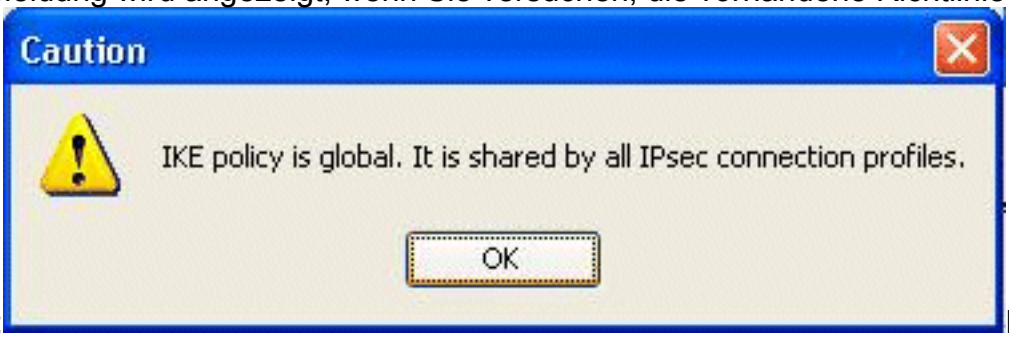


8. Klicken Sie auf **Verwalten...** um die IKE-Richtlinie zu
ändern.



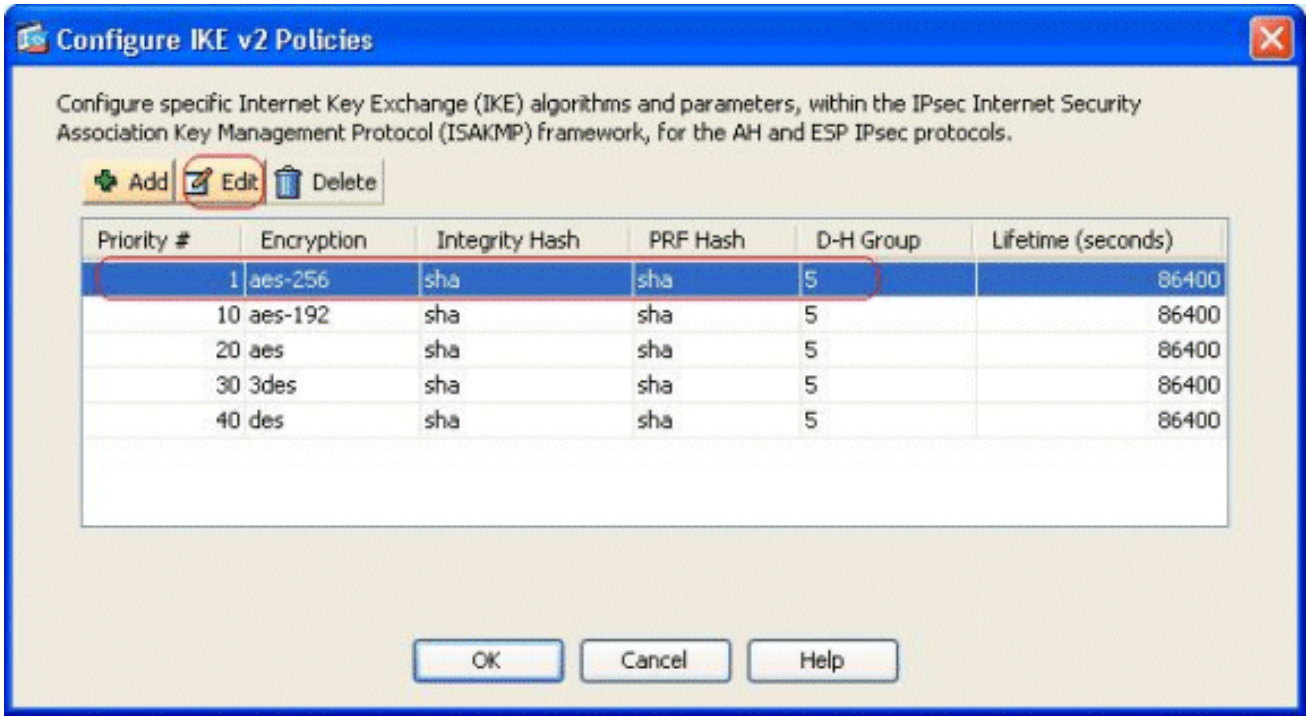
Hinweis: IKE-Richtlinie in IKEv2 ist gleichbedeutend mit der **ISAKMP-Richtlinie** in IKEv1.**Der IPsec-Vorschlag** in IKEv2 ist gleichbedeutend mit dem **Transform Set** in IKEv1.

9. Diese Meldung wird angezeigt, wenn Sie versuchen, die vorhandene Richtlinie zu ändern:



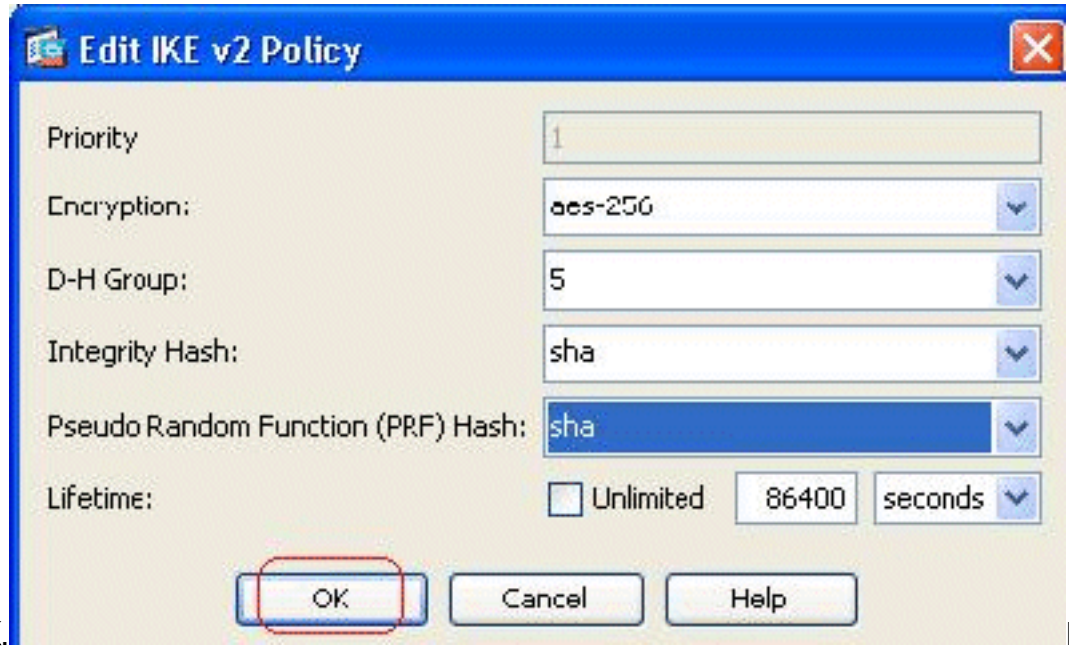
Klicken Sie auf **OK**, um fortzufahren.

10. Wählen Sie die angegebene IKE-Richtlinie aus, und klicken Sie auf **Bearbeiten**.



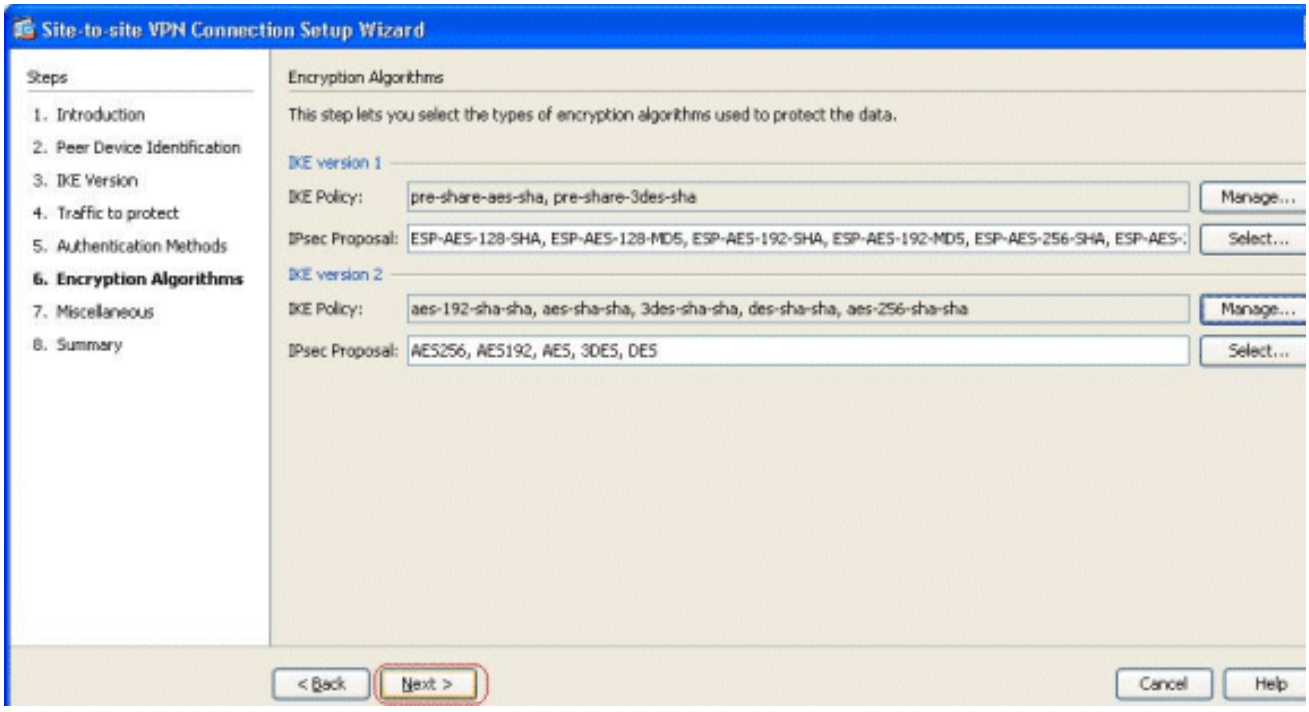
11. Sie können die Parameter wie Priority, Encryption, D-H Group, Integrity Hash, PRF Hash

und Lifetime-Werte ändern. Klicken Sie abschließend auf



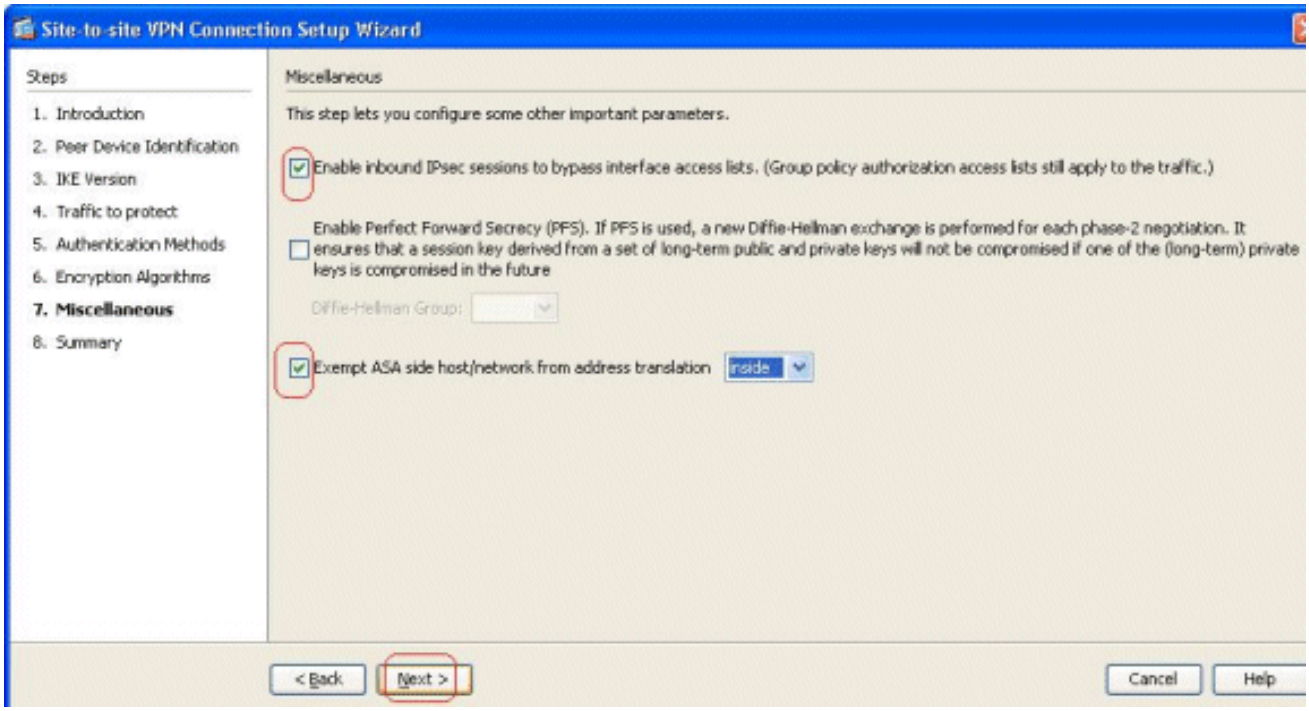
OK. IKEv2 ermöglicht die getrennte Aushandlung des Integrity-Algorithmus vom Pseudo Random Function (PRF)-Algorithmus. Dies kann in der IKE-Richtlinie konfiguriert werden, wobei die aktuell verfügbaren Optionen SHA-1 oder MD5 sind.Sie können die standardmäßig definierten IPsec-Angebotsparameter nicht ändern. Klicken Sie neben dem Feld "IPsec Proposal" (IPsec-Angebot) auf **Select** (**Auswählen**), um neue Parameter hinzuzufügen. Der Hauptunterschied zwischen IKEv1 und IKEv2 besteht im Hinblick auf die IPsec-Vorschläge darin, dass IKEv1 das Transformationssatz in Kombinationen von Verschlüsselungs- und Authentifizierungsalgorithmen akzeptiert. IKEv2 akzeptiert die Verschlüsselungs- und Integritätsparameter einzeln und ermöglicht letztendlich alle ODER Kombinationen dieser Parameter. Sie können diese am Ende dieses Assistenten auf der Folie Zusammenfassung anzeigen.

12. Klicken Sie auf **Weiter**.

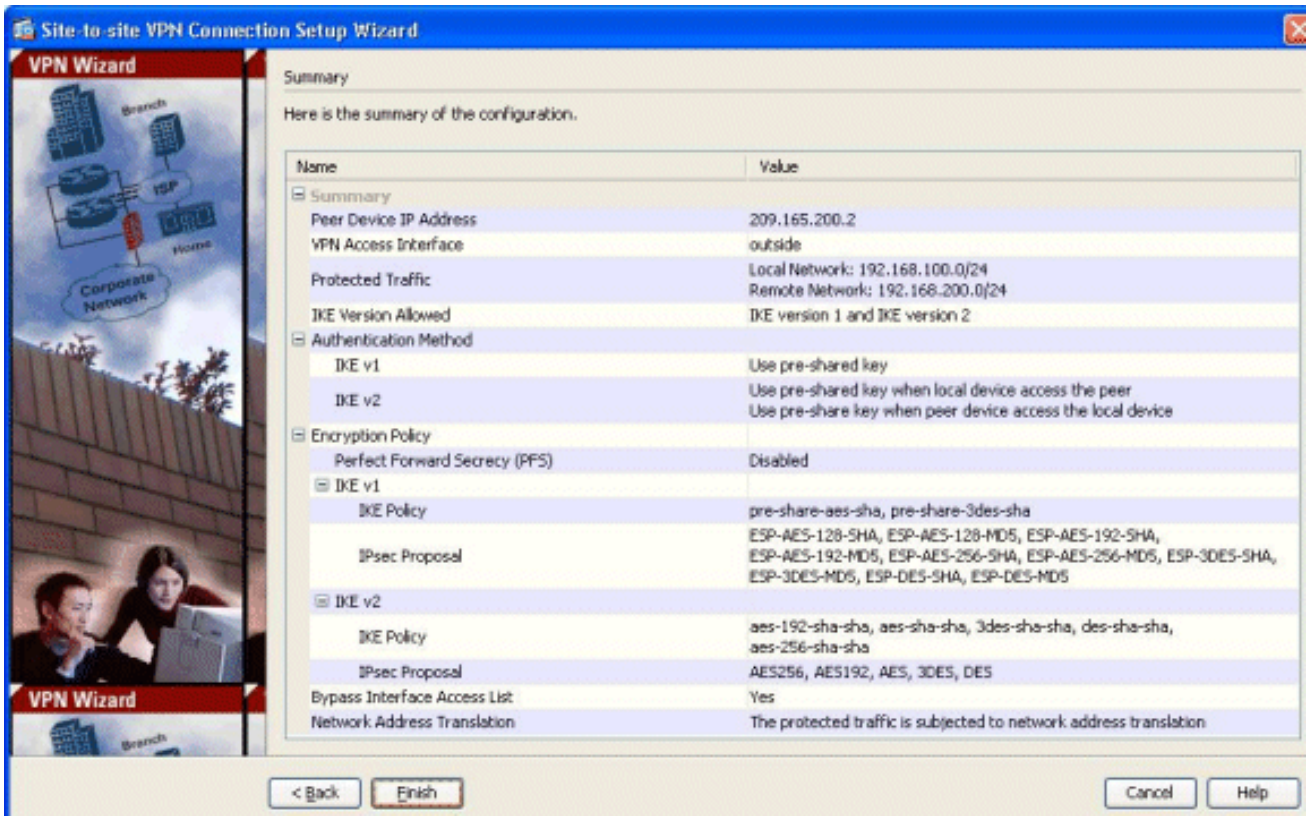


13. Geben Sie die Details an, z. B. NAT-Freistellung, PFS und die Umgehung von Schnittstellen-ACLs. Wählen Sie **Weiter**

aus.



14. Eine Zusammenfassung der Konfiguration finden Sie hier:



Klicken Sie auf **Fertig stellen**, um den Site-to-Site VPN-Tunnel-Assistenten abzuschließen. Ein neues Verbindungsprofil wird mit den konfigurierten Parametern erstellt.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- show crypto ikev2 sa - Zeigt die SA-Datenbank der IKEv2-Laufzeit an.
- show vpn-sessiondb detail l2l: Zeigt Informationen über Site-to-Site-VPN-Sitzungen an.

Fehlerbehebung

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- debug crypto ikev2 - Zeigt **Debug-**Nachrichten für IKEv2 an.

Zugehörige Informationen

- Technischer Support für Cisco Appliances der Serie ASA 5500
- Technischer Support und Dokumentation - Cisco Systems