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

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Konfigurieren Netzwerkdiagramm ASDM-Konfiguration auf Hauptsitz-ASA Überprüfen Fehlerbehebung Befehle zur Fehlerbehebung Zugehörige Informationen

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

<u>Anforderungen</u>

Stellen Sie sicher, dass die Cisco ASA mit den <u>Grundeinstellungen</u> 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 <u>Cisco Technical Tips</u> <u>Conventions</u> (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 <u>Command Lookup Tool</u> (nur <u>registrierte</u> 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.

Home 🖧 Cor	Startup Wizard	n 🙆 Back 🎒 Forward 🦻 Help
Deutice List	VPN Wizards	Site-to-site VPN Wizard
Add Delete	High Availability and Scalability Wizard Unified Communication Wizard Restart Centure Wizard	AnyConnect VPN Wizard Clientless SSL VPN Wizard

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

📬 Site-to-site VPN Connecti	on Setup Wizard
Site-to-site VPN Connection	Introduction Use this wizard to setup new site-to-site VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol. Site-to-Site VPN Local Remote Remote Remote Remote Remote Remote Remote Remote Remote Remote Remote Remote Remote
	<back next=""> Cancel He</back>

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

🐔 Site-to-site VPN Connec	tion Setup Wizard			
Steps	Peer Device Identificat	tion		
1. Introduction	This step lets you iden	tify the peer VPN device by its IP address	and the interface used to access the peer.	
2. Peer Device Identification	Peer IP Address:	209.165.200.2		
3. IKE Version				
4. Traffic to protect	VPN Access Interface:	outside	~	
5. Authentication Methods				
6. Encryption Algorithms				
7. Miscellaneous				
8. Summary				
	< Back Next >			Cancel Help

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

🚳 Site-to-site VPN Connect	ion Setup Wizard
Site-to-site VPN Connect Steps 1. Introduction 2. Peer Device Identification 3. IKE Version 4. Traffic to protect 5. Authentication Methods 6. Encryption Algorithms 7. Miscellaneous 8. Summary	ion Setup Wizard IKE Version ASA supports both version 1 and version 2 of the IKE (Internet Key Exchange) protocol. This step lets you decide which version or versions to support in this connection profile. IV IKE version 1 IV IKE version 2
	< Back (Next >) Cancel (Help

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

Steps	Traffic to protect
 Introduction Peer Device Identification IKE Version Traffic to protect Authentication Methods Encryption Algorithms Miscellaneous Summary 	This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption. IP Address Type: IPv4 IPv6 Local Network: 192.168.100.0/24 Remote Network: 192.168.200.0/24

an.

teps	Authentication Methods			
 Introduction Peer Device Identification IKE Version 	This step lets you configure the methods INE version 1 Pre-shared Key:	s to authenticate with the peer d	evice.	
 Traffic to protect Authentication Methods Encryptico Algorithms 	Device Certificate: DRE version 2	None	~	Manage
7. Miscellaneous 8. Summary	C Local Device Certificate: Remote Peer Pre-shared Key:	None	~	Manage
	Remote Peer Certificate Authentication:	Allowed		Manage

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:

🚳 Site-to-site VPN Connect	ion Setup Wizar	rd	E
Steps	Encryption Algori	tims	
 Introduction Peer Device Identification IKE Version Traffic to protect Authentication Methods 	This step lets you IKE version 1 — IKE Policy: IPsec Proposal:	u select the types of encryption algorithms used to protect the data. pre-share-aes-sha, pre-share-3des-sha ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-2	Manage Select
6. Encryption Algorithms	IKE version 2 -		
7. Miscellaneous	DKE Policy:	aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha	Manage
8. Summary	IPsec Proposal:	AES256, AES192, AE5, 3DE5, DE5	Select
	< Back	Jest > Cancel	Help

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

Steps	noryption Algorithms	
Introduction Peer Device Identification IKE Version Traffic to protect Authentication Methods Encryption Algorithms	is step lets you select the types of encryption algorithms used to protect the data. E version 1 E Policy: pre-share-aes-sha, pre-share-3des-sha sec Proposal: ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-1 E version 2	92-MD5, ESP-AES-256-SHA, ESP-AES- Select
6. Encryption Algorithms 7. Miscelaneous 8. Summary	E Policy: aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des sec Proposal: AES256, AE5192, AES, 3DE5, DE5	-sha-sha Manage Select

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



auf **OK**, um fortzufahren.

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

Bearbeiten.

Priority #	Encryption	Integrity Hash	PRF Hash	D-H Group	Lifetime (seconds)
	1 aes-256	sha	sha	5	8640
1	10 aes-192	sha	sha	5	8640
2	20 aes	sha	sha	5	8640
3	30 3des	sha	sha	5	8640
	10 des	sha	sha	5	8640

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

und Lifetime-Werte ändern. Klicken Sie abschließend auf

Priority	1	
Encryption:	aes-256	*
D-H Group:	5	~
Integrity Hash:	sha	~
Pseudo Random Function (PRF) Hash:	sha	~
Lifetime:	Unlimited 86400 seconds	~

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.

🛍 Site-to-site VPN Connect	ion Setup Wizard
Steps	Encryption Algorithms
 Introduction Peer Device Identification IXE Version Traffic to protect Authentication Methods 	This step lets you select the types of encryption algorithms used to protect the data. IXE version 1 IXE Policy: pre-share-aes-sha, pre-share-3des-sha IPsec Proposal: ESP-AES-128-MD5, ESP-AES-192-MD5, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-:
 Encryption Algorithms Miscelaneous Summery 	INE version 2 INE Policy: aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha, aes-256-sha-sha IPsec Proposal: AES256, AES192, AES, 3DES, DES Select Select
	< Back Next > Cancel Help

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

aus.

📬 Site-to-site VPN Connec	tion Setup Wizard	
Steps	Niscelaneous	
 Introduction Peer Device Identification IKE Version Traffic to protect Authentication Methods Encryption Algorithms Miscellaneous Summary 	This step lets you configure some other important parameters.	be
	< Back [Next >] Cancel Help	_

14. Eine Zusammenfassung der Konfiguration finden Sie

Summary	
Here is the summary of the configuration.	
Name	Value
Summary	
Peer Device IP Address	209.165.200.2
VPN Access Interface	outside
Protected Traffic	Local Network: 192.168.100.0/24 Remote Network: 192.168.200.0/24
IKE Version Allowed	IKE version 1 and IKE version 2
Authentication Method	
IKE v1	Use pre-shared key
D/E v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
BKE v1	
IKE Policy	pre-share-aes-sha, pre-share-3des-sha
IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DE5-SHA, ESP-3DE5-MD5, ESP-DE5-SHA, ESP-DE5-MD5
■ IKE v2	
IKE Policy	aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha, aes-256-sha-sha
IPsec Proposal	AES256, AES192, AES, 3DES, DES
Bypass Interface Access List	Yes
Network Address Translation	The protected traffic is subjected to network address translation

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

<u>Überprüfen</u>

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

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> 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 121: Zeigt Informationen über Site-to-Site-VPN-Sitzungen an.

Fehlerbehebung

Befehle zur Fehlerbehebung

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

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

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

Zugehörige Informationen

- Technischer Support für Cisco Appliances der Serie ASA 5500
- <u>Technischer Support und Dokumentation Cisco Systems</u>