ASDM 6.4: Esempio di configurazione del tunnel VPN da sito a sito con IKEv2

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Configurazione Esempio di rete Configurazione ASDM su HQ-ASA Verifica Risoluzione dei problemi Comandi per la risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritto come configurare un tunnel VPN da sito a sito tra due appliance Cisco Adaptive Security Appliance (ASA) utilizzando Internet Key Exchange (IKE) versione 2. Viene descritta la procedura utilizzata per configurare il tunnel VPN con una GUI guidata di Adaptive Security Device Manager (ASDM).

Prerequisiti

Requisiti

Verificare che Cisco ASA sia stato configurato con le impostazioni di base.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA serie 5500 Adaptive Security Appliance con software versione 8.4 e successive
- Software Cisco ASDM versione 6.4 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Premesse

IKEv2 è un miglioramento del protocollo IKEv1 esistente che include i seguenti vantaggi:

- Meno scambi di messaggi tra peer IKE
- Metodi di autenticazione unidirezionale
- Supporto integrato per Dead Peer Detection (DPD) e NAT-Traversal
- Utilizzo del protocollo EAP (Extensible Authentication Protocol) per l'autenticazione
- Eliminazione del rischio di attacchi DoS semplici mediante l'utilizzo di cookie anti-clogging

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



In questo documento viene illustrata la configurazione del tunnel VPN da sito a sito su HQ-ASA. La stessa operazione può essere eseguita anche come mirror sull'appliance BQ-ASA.

Configurazione ASDM su HQ-ASA

Questo tunnel VPN può essere configurato usando una semplice procedura guidata GUI.

Attenersi alla seguente procedura:

1. Accedere ad ASDM e selezionare **Wizards > VPN Wizard > Site-to-site VPN Wizard** (Procedure guidate

VPN).

File View Tools	Wizards Window Help	
Home & Cor	Startup Wizard	Back C Forward 9 Help
Daulsa List	VPN Wizards	Site-to-site VPN Wizard
Add Delete	High Availability and Scalability Wizard Unified Communication Wizard	AnyConnect VPN Wizard Clientless SSL VPN Wizard
Find:	Packet Capture Wizard	IPsec (IKEv1) Remote Access VPN Wizard

2. Viene visualizzata una finestra di impostazione della connessione VPN da sito a sito. Fare clic su Next

(Avanti).	
🖀 Site-to-site VPN Connecti	ion Setup Wizard
VPN Wizard	Introduction
and a second	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.
	< Back Next > Cancel He

3. Specificare l'indirizzo IP peer e l'interfaccia di accesso VPN. Fare clic su **Next** (Avanti).

tion Setup Wizard			E
Peer Device Identification			
This step lets you identify Peer IP Address: 20 VPN Access Interface: 0	the peer VPN device by its IP address an 19.165.200.2	nd the interface used to access the peer.	
< Back Next >)		Cancel Help
	tion Setup Wizard Peer Device Identification This step lets you identify Peer IP Address: [2] VPN Access Interface: [0] <	tion Setup Wizard Peer Device Identification This step lets you identify the peer VPN device by its IP address a Peer IP Address: 209.165.200.2 VPN Access Interface: Outside	Setup Wizard Peer Device Identification This step lets you identify the peer VPN device by its IP address and the interface used to access the peer. Peer IP Address: 209.165.200.2 WPN Access Interface: outside VPN Access Interface: v

4. Selezionare entrambe le versioni IKE e fare clic su **Avanti**.

🚳 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	INE 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. INE version 1 INE version 2 INE version 2
	< Back Next > Cancel Help

Nota: entrambe le versioni di IKE sono configurate qui perché l'iniziatore potrebbe avere un backup da IKEv2 a IKEv1 quando si verifica un errore di IKEv2.

5. Specificare la rete locale e la rete remota in modo che il traffico tra queste reti venga crittografato e passato attraverso il tunnel VPN. Fare clic su **Next** (Avanti).

Steps	Traffic to protect
1. Introduction 2. Peer Device Identification 3. IXE Version 4. Traffic to protect 5. Authentication Methods 6. Encryption Algorithms 7. Miscellaneous 8. 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: I92.168.100.0/24 I92.168.200.0/24 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII

6. Specificare le chiavi già condivise per entrambe le versioni di IKE.

eps	Authentication Methods			
. Introduction . Peer Device Identification . IXE Version . Traffic to protect	This step lets you configure the methods IKE version 1 Pre-shared Key: During CathEnder	to authenticate with the peer d	evice.	Harra
Authentication Methods Encryption Algorithms	IXE version 2	·····		manage
. Miscellaneous . Summary	Local Device Certificate: Remote Peer Pre-shared Key:	None	~	Manage
	Remote Peer Certificate Authentication:	Allowed		Manage

La differenza principale tra IKE versioni 1 e 2 consiste nel metodo di autenticazione consentito. IKEv1 consente un solo tipo di autenticazione a entrambi i terminali della VPN (chiave precondivisa o certificato). Tuttavia, IKEv2 consente di configurare i metodi di autenticazione asimmetrica (ovvero l'autenticazione con chiave precondivisa per il mittente, ma l'autenticazione del certificato per il risponditore) utilizzando CLI di autenticazione locale e remota separate.Inoltre, è possibile avere diverse chiavi già condivise su entrambe le estremità. La chiave locale pre-condivisa all'estremità HQ-ASA diventa la chiave remota pre-condivisa sull'estremità HQ-ASA.

7. Specificare gli algoritmi di crittografia per IKE versioni 1 e 2. I valori predefiniti sono accettati:

Reps	Encryption Algor	ithms	
Introduction Peer Device Identification If Version Traffic to protect Authentication Methods Encryption Algorithms Miscellaneous Summary	This step lets yo IKE version 1 — IKE Policy: IPsec Proposal: IKE version 2 — IKE Policy: IPsec Proposal: 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-MD6, ESP-AES-256-SHA, ESP-AES- aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha AES256, AES192, AES, 3DES, DES	Manage Select Manage Select

8. Per modificare il criterio IKE, fare clic su **Gestisci**...

1. Introduction This step lets you select the types of encryption algorithms used to protect the data. 2. Peer Device Identification Intervention 3. IKE Version Intervention 4. Traffic to protect Intervention 5. Authentication Methods IPsec Proposal: 6. Encryption Algorithms INtervention 2 7. Miscellaneous INte Policy: 8. Summary IPsec Proposal: 9. Segregation AES256, AES192, AES, 30ES, 0ES	
	Manage Select Manage Select

Nota: Il criterio IKE in IKEv2 è sinonimo del criterio ISAKMP in IKEv1.Proposta IPSec in IKEv2 è sinonimo di Trasformazione impostata in IKEv1.

9. Questo messaggio viene visualizzato quando si tenta di modificare il criterio



esistente:

continuare, fare clic su OK.

10. Selezionare il criterio IKE specificato e fare clic su

Modifica.

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

11. Èpossibile modificare parametri quali Priorità, Crittografia, Gruppo D-H, Hash di integrità,

Hash PRF e Valori di durata. Al termine, fare clic su

Priority	1	
Encryption:	aes-250	¥
D-H Group:	5	~
Integrity Hash:	sha	~
Pseudo Random Function (PRF) Hash:	sha	~
Lifetime:	Unlimited 86400 seconds	~

consente di negoziare l'algoritmo Integrity separatamente dall'algoritmo PRF (Pseudo Random Function). È possibile configurare questa opzione nel criterio IKE con le opzioni disponibili correnti SHA-1 o MD5.Non è possibile modificare i parametri della proposta IPSec definiti per impostazione predefinita. Per aggiungere nuovi parametri, fare clic su **Select** (Seleziona) accanto al campo IPsec Project (Proposta IPSec). La differenza principale tra IKEv1 e IKEv2, in termini di proposte IPsec, è che IKEv1 accetta la trasformazione impostata in termini di combinazioni di algoritmi di crittografia e autenticazione. IKEv2 accetta i parametri di crittografia e integrità singolarmente e rende infine possibili tutte le combinazioni di parametri OR. È possibile visualizzarli al termine della procedura guidata nella diapositiva Riepilogo.

12. Fare clic su Next

(Avanti).

Steps	Encryption Algori	thms	
1. Introduction 2. Peer Device Identification 3. IKE Version 4. Traffic to protect 5. Authentication Methods 6. Encryption Algorithms 7. Miscellaneous 8. Summary	Encryption Augor This step lets you IKE version 1 — IKE Policy: IPsec Proposal: IKE version 2 — IKE Policy: IPsec Proposal:	I 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-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-: aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha, aes-256-sha-sha AES256, AES192, AES, 3DES, DES	Manage Select Manage Select

 Specificare i dettagli, ad esempio l'esenzione NAT, PFS e il bypass dell'ACL di interfaccia. Scegliere

Successivo.

📬 Site-to-site VPN Connect	lion Setup Wizard	
Steps	Miscellaneous	
 Introduction Peer Device Identification IKE Version Traffic to protect Authentication Methods Encryption Algorithms Miscellaneous Summary 	This step lets you configure some other important parameters.	te
	< Back Next > Cancel Help	

14. Di seguito è riportato un riepilogo della configurazione:

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
IKE 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
E IKE 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-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
BKE 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	Ves
Network Address Translation	The protected traffic is subjected to network address translation

Per completare la procedura guidata del tunnel VPN da sito a sito, fare clic su **Fine**. Viene creato un nuovo profilo di connessione con i parametri configurati.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- show crypto ikev2 sa: visualizza il database SA di runtime IKEv2.
- show vpn-sessiondb detail 121: visualizza le informazioni sulle sessioni VPN da sito a sito.

Risoluzione dei problemi

Comandi per la risoluzione dei problemi

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

• debug crypto ikev2: visualizza i messaggi di debug per IKEv2.

Informazioni correlate

- <u>Appliance Cisco ASA serie 5500 Supporto tecnico</u>
- Documentazione e supporto tecnico Cisco Systems