ASDM 6.4: Túnel do VPN de Site-para-Site com exemplo de configuração IKEv2

Índice

Introdução Pré-requisitos Requisitos Componentes Utilizados Convenções Informações de Apoio Configurar Diagrama de Rede Configuração ASDM em HQ-ASA Verificar Troubleshooting Comandos para Troubleshooting Informações Relacionadas

Introdução

Este documento descreve como configurar um túnel VPN de site a site entre duas Cisco Adaptive Security Appliances (ASAs) que usam Internet Key Exchange (IKE) versão 2. Ele descreve as etapas usadas para configurar o túnel VPN usando um assistente de GUI do Adaptive Security Device Manager (ASDM).

Pré-requisitos

Requisitos

Certifique-se de que Cisco ASA esteve configurado com as configurações básicas.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivos de segurança adaptáveis Cisco ASA série 5500 que executa a versão de software 8.4 e mais atrasado
- Versão 6.4 e mais recente do software ASDM de Cisco

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as <u>Convenções de Dicas Técnicas da Cisco</u> para obter mais informações sobre convenções de documentos.

Informações de Apoio

IKEv2, é um realce ao protocolo IKEv1 existente que inclui estes benefícios:

- Menos trocas da mensagem entre pares IKE
- Métodos de autenticação unidirecional
- Suporte embutido para o Dead Peer Detection (DPD) e o NAT-Traversal
- Uso do Extensible Authentication Protocol (EAP) para a autenticação
- Elimina o risco de ataques simples DoS usando Cookie antiobstrução

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a <u>Command Lookup Tool</u> (<u>somente clientes registrados</u>) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Este documento mostra a configuração do túnel do VPN de Site-para-Site em HQ-ASA. O mesmos podiam ser seguidos que um espelho no BQ-ASA.

Configuração ASDM em HQ-ASA

Este túnel VPN podia ser configurado usando um assistente fácil de usar GUI.

Conclua estes passos:

1. Entre ao ASDM, e vá aos assistentes > aos wizard VPN > ao assistente do VPN de Site-

para-Site

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

2. Um indicador da instalação de conexão do VPN de Site-para-Site aparece. Clique em Next.

🗃 Site-to-site VPN Connectio	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 Local Remote Local Local
	< Back Next > Cancel Hel

3. Especifique o endereço IP do peer e a interface de acesso VPN. Clique em Next

NEXI.			
🐔 Site-to-site VPN Conner	tion Setup Wizard		
Steps 1. Introduction 2. Peer Device Identification 3. IKE Version 4. Traffic to protect	Peer Device Identification This step lets you identify the peer VPN device by its IP address and the interf Peer IP Address: 209.165.200.2 VPN Access Interface: outside	ace used to access the peer.	
 Authentication Methods Encryption Algorithms Miscellaneous Summary 			
	< Back Next >	Cancel	Help

4. Selecione ambas as versões IKE, e clique-as **em seguida**.

🚳 Site-to-site VPN Connect	ion Setup Wizard
Site-to-site VPN Connect Steps I. Introduction Peer Device Identification IKE Version Traffic to protect Authentication Methods Encryption Algorithms Miscellaneous 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
	< Back Next > Cancel Help

Nota: Ambas as versões do IKE são configuradas aqui porque o iniciador poderia ter um backup de IKEv2 a IKEv1 quando IKEv2 falha.

5. Especifique a rede local e a rede remota de modo que o tráfego entre estas redes seja cifrado e passado através do túnel VPN. Clique em Next

Reps	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: I92.168.100.0/24 IPv6 IPv6 IPv6 IPv6 IPv6 IPv6 IPv6 IPv6

6. Especifique as chaves pré-compartilhada para ambas as versões do IKE.

Introduction Peer Device Identification	This step lets you configure the methods	to authenticate with the peer de	vice.	
. IKE Version	DKE version 1 Pre-shared Key:			
Authentication Methods Encryption Algorithms	Device Certificate: DKE version 2 (a) Local Pre-shared Key:	None		Manage
. Miscellaneous . Summary	Local Device Certificate: Remote Peer Pre-shared Key:	None	~	Manage
	Remote Peer Certificate Authentication:	Allowed		Manage

A diferença principal entre versões 1 e 2 IKE encontra-se em termos do método de autenticação que permitem. IKEv1 permite somente um tipo de autenticação em ambas as extremidades VPN (isto é, chave pré-compartilhada ou certificado). Contudo, IKEv2 permite que os métodos de autenticação assimétricos sejam configurados (isto é, autenticação da chave pré-compartilhada para o autor, mas certificado de autenticação para o que responde) usando o local separado e a autenticação remota CLI.Mais, você pode ter chaves pré-compartilhada diferentes no ambas as extremidades. A chave pré-compartilhada local na extremidade HQ-ASA transforma-se a chave pré-compartilhada remota na extremidade BQ-ASA. Igualmente, a chave pré-compartilhada remota na extremidade BQ-ASA.

7. Especifique os algoritmos de criptografia para ambas as versões 1 e 2 IKE. Aqui, os valores padrão são

aceitados:

Steps	Encryption Algorit	thms	
Introduction Peer Device Identification IXE Version Traffic to protect Authentication Methods Encounting Algorithms	This step lets you DKE version 1 DKE Policy: DPsec Proposal: DKE version 2	e 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-	Manage. Select
6. Encryption Algorithms 7. Miscellaneous 8. Summary	IKE Policy:	aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha AES256, AES192, AES, 3DES, DES	Manage. Select.,

8. O clique controla... a fim alterar a política de

I	K	Е
		_

🚳 Site-to-site VPN Connect	tion Setup Wizard	
Steps 1. Introduction 2. Peer Device Identification 3. IKE Version	Encryption Algorithms This step lets you select the types of encryption algorithms used to protect the data. DKE version 1 DKE Relicu	
 Traffic to protect Authentication Methods Encryption Algorithms 	IPsec Proposali ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES- IKE version 2	
7. Miscellaneous 8. Summary	IKE Policy: aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha Manag IPsec Proposal: AES256, AES192, AES, 3DES, DES Select	e
	< Back Next > Cancel H	elp

Nota: A política de IKE em IKEv2 é sinônima à política de ISAKMP em IKEv1. A proposta do IPsec em IKEv2 é sinônima à transformação ajustada em IKEv1.

9. Esta mensagem aparece quando você tenta alterar a política



existente:

O do clique a fim continuar.

10. Selecione a política de IKE especificada, e o clique

edita.

Priority #	Encryption	Integrity Hash	PRF Hash	D-H Group	Lifetime (seconds)
C. States	1 aes-256	sha	sha	5	86400
1	10 aes-192	sha	sha	5	86400
2	20 aes	sha	sha	5	86400
3	30 3des	sha	sha	5	86400
	10 des	sha	sha	5	86400
			Caracter of C		

11. Você pode alterar os parâmetros tais como a prioridade, a criptografia, o grupo do D-H, a mistura da integridade, da mistura PRF valores, e da vida. **APROVAÇÃO do** clique quando

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

terminado.

IKEv2

permite o algoritmo da integridade ser negociado separadamente do algoritmo aleatório pseudo- da função (PRF). Isto podia ser configurado na política de IKE com as opções disponíveis atuais que são SHA-1 ou MD5.Você não pode alterar os parâmetros da proposta do IPsec que são definidos à revelia. Clique **seleto** ao lado do campo da proposta do IPsec a fim adicionar parâmetros novos. A diferença principal entre IKEv1 e IKEv2, em termos das propostas do IPsec, é que IKEv1 aceita a transformação ajustada em termos das combinações de criptografia e de algoritmos de autenticação. IKEv2 aceita os parâmetros da criptografia e da integridade individualmente, e faz finalmente todo o possível OU combinações destes. Você poderia ver estes na extremidade deste assistente, na corrediça sumária.

12. Clique em

Next.

🛍 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. INE version 1 INE Policy: pre-share-ass-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-SHA, ESP-AES-128-MD5, ESP-AES-192-MD5, ESP-AES-256-SHA,
 Encryption Algorithms Miscelaneous Summary 	DKE version 2 DKE Policy: aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha, aes-256-sha-sha DPsec Proposal: AES256, AES192, AE5, 3DE5, DE5 Select
	< Back Next > Cancel Help

13. Especifique os detalhes, tais como a isenção de NAT, o PFS, e contornear da relação ACL. Escolha **em**

seguida.

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

14. Um sumário da configuração pode ser considerado

Summary	
Branch Here is the summary of the configuration.	
Name	Value
E 10 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-3DE5-SHA, ESP-3DE5-MD5, ESP-DE5-SHA, ESP-DE5-MD5
INE 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

Revestimento do clique a fim terminar o assistente do túnel do VPN de Site-para-Site. Um perfil da nova conexão é criado com os parâmetros configurados.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A <u>Output Interpreter Tool</u> (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- mostre ikev2 criptos sa Indica IKEv2 o base de dados tempo de execução SA.
- mostre VPN-sessiondb o detalhe I2I Indica a informação sobre sessões do VPN de Sitepara-Site.

Troubleshooting

Comandos para Troubleshooting

A <u>Output Interpreter Tool</u> (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte <u>Informações Importantes sobre Comandos de Depuração</u> antes de usar comandos **debug**.

• <u>debug crypto ikev2</u> - As mostras debugam mensagens para IKEv2.

Informações Relacionadas

- Suporte técnico dos dispositivos do 5500 Series de Cisco ASA
- <u>Suporte Técnico e Documentação Cisco Systems</u>