SDM: IPSec local a local VPN entre ASA/PIX e um exemplo de configuração do IOS Router

Índice

Introdução

Este documento fornece uma configuração de exemplo para o túnel de IPsec do LAN a LAN (Site a site) entre os Cisco Security Appliances (ASA/PIX) e o Cisco IOS Router. As rotas estáticas são usadas por simplicidade.

Refira a ferramenta de segurança PIX/ASA 7.x a um exemplo de configuração do túnel IPSec de LAN para LAN do IOS Router a fim aprender uma encenação mais mais ou menos idêntica onde a ferramenta de segurança PIX/ASA execute a versão de software *7.x*.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- A conectividade IP fim-a-fim deve ser estabelecida antes de começar esta configuração.
- A licença da ferramenta de segurança deve ser permitida para a criptografia do Data

Encryption Standard (DES) (a nível mínimo da criptografia).

Componentes Utilizados

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

- Ferramenta de segurança adaptável de Cisco (ASA) com versão 8.x e mais recente
- Versão 6.x.and ASDM mais atrasada
- Cisco 1812 Router com Software Release 12.3 de Cisco IOS®
- Versão 2.5 do gerenciador do dispositivo de segurança da Cisco (SDM)

Nota: Consulte Habilitação de Acesso HTTPS para o ASDM para permitir que o ASA seja configurado pelo ASDM.

Nota: Refira a configuração de roteador básico usando o SDM a fim permitir que o roteador seja configurado pelo SDM.

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.

Nota: Refira o profissional da configuração: IPSec local a local VPN entre ASA/PIX e um exemplo de configuração do IOS Router para uma configuração similar usando o Cisco Configuration Professional no roteador.

Produtos Relacionados

Esta configuração pode igualmente ser usada com a ferramenta de segurança da série do Cisco PIX 500, que executa a versão 7.x e mais recente.

Convenções

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

Configuração

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.

Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918, que foram usados em um ambiente de laboratório.

- Configuração ASDM do túnel VPN
- Configuração de SDM do roteador
- Configuração do ASA via CLI
- Configuração de CLI do roteador

Configuração ASDM do túnel VPN

Termine estas etapas a fim criar o túnel VPN:

1. Abra seu navegador e incorpore **<IP_Address de https:// da relação do ASA que foi configurado para ASDM Access>** para alcançar o ASDM no ASA.Certifique-se autorizar todos os avisos que seu navegador o der relativo à autenticidade de certificado de SSL. O nome de usuário padrão e a senha são ambos placa.O ASA apresenta este indicador para permitir a transferência do aplicativo ASDM. Este exemplo carrega o aplicativo no computador local e não o é executado em um Java applet.
2. Clique a **launcher ASDM da transferência e comece o ASDM** a fim transferir o instalador para o aplicativo ASDM.
3. Uma vez as transferências da launcher ASDM, terminam as etapas dirigidas pelas alertas a fim instalar o software e executar o lançador ASDM Cisco.
4. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT para a relação que você configurou com o **HTTP -** comande, e um nome de usuário e senha se você especificou um.Este exemplo usa o **cisco123** para o username e o **cisco123** como a senha.
5. Execute o **assistente do IPSec VPN** uma vez que o aplicativo ASDM conecta ao ASA.
6. Escolha o tipo de túnel do **IPSec local a local** VPN e clique-o **em seguida** como mostrado aqui.
7. Especifique o endereço IP externo do peer remoto. Incorpore a informação da autenticação para usar-se, que é a chave pré-compartilhada neste exemplo. A chave pré-compartilhada usada neste exemplo é **cisco123**. **O nome de grupo de túneis** será seu endereço IP externo à revelia se você configura L2L VPN. Clique em Next.
8. Especifique os atributos para usar-se para o IKE, igualmente sabido como a fase 1. Estes atributos devem ser os mesmos no ASA e no IOS Router. Clique em Next.
9. Especifique os atributos para usar-se para o IPsec, igualmente sabido como a fase 2. Estes atributos devem combinar no ASA e no IOS Router. Clique em Next.
10. Especifique os anfitriões cujo o tráfego deve ser permitido passar através do túnel VPN. Nesta etapa, você tem que fornecer as **redes remotas e locais** para o túnel VPN. Clique o botão ao lado das **redes local** como mostrado aqui para escolher para baixo o endereço de rede local da lista de gota.
11. Escolha o endereço de **rede local**, a seguir clique a **APROVAÇÃO** como mostrado aqui.
12. Clique o botão ao lado das **redes remotas** como mostrado aqui para escolher para baixo o endereço de rede remota da lista de gota.
13. Escolha o endereço de **rede remota**, a seguir clique a **APROVAÇÃO** como mostrado aqui.**Nota:** Se você não tem a rede remota na lista então a rede tem que ser adicionada à lista clicando **adiciona**.
14. Verifique o **host/rede isentos do lado ASA da** caixa de seleção da **tradução de endereços** a fim impedir que o tráfego de túnel se submeta à **tradução de endereço de rede**. Então, clique **em seguida**.
15. Os atributos definidos pelo wizard VPN são indicados neste sumário. Verifique novamente a configuração e clique o **revestimento** quando você é satisfeito os ajustes está correto.

Configuração de SDM do roteador

Termine estas etapas a fim configurar o túnel do VPN de Site-para-Site no roteador do Cisco IOS:

1. Abra seu navegador e incorpore **<IP_Address de https:// da relação do roteador que foi configurado para SDM Access>** para alcançar o SDM no roteador.Certifique-se autorizar todos os avisos que seu navegador o der relativo à autenticidade de certificado de SSL. O nome de usuário padrão e a senha são ambos placa.O roteador apresenta este indicador para permitir a transferência do aplicativo SDM. Este exemplo carrega o aplicativo no computador local e não o é executado em um Java applet.
2. A transferência SDM começa agora. Uma vez as transferências do lançador SDM, terminam as etapas dirigidas pelas alertas a fim instalar o software e executar o lançador de Cisco SDM.
3. Incorpore o **nome de usuário e senha** se você especificou um e clica a **APROVAÇÃO**.Este exemplo usa o **cisco123** para o username e o **cisco123** como a senha.
4. Escolha **Configuration->VPN->Site-to-Site VPN** e clique o botão de rádio ao lado de **criam um VPN de Site-para-Site no** Home Page SDM. Então, **lançamento do** clique a **tarefa selecionada** como mostrado aqui:
5. Escolha o **assistente passo a passo** continuar com a configuração:
6. Na próxima janela forneça a **informação da conexão de VPN nos** espaços respectivos. Selecione a relação do túnel VPN da lista de gota para baixo. Aqui, **FastEthernet0** é escolhido. Na seção da **identidade do par**, escolha o **par com endereço IP estático** e forneça o endereço IP de Um ou Mais Servidores Cisco ICM NT do peer remoto. Então, forneça a **chave pré-compartilhada** (**cisco123 n**este exemplo) na seção da autenticação como mostrado. Então, clique **em seguida**.
7. O clique **adiciona** para adicionar propostas IKE que especifica o **algoritmo de criptografia, o algoritmo de autenticação** e o **método das trocas de chave**.
8. Forneça o **algoritmo de criptografia**, o **algoritmo de autenticação** e o **método das trocas de chave** como mostrado aqui, a seguir clique a **APROVAÇÃO**. **O algoritmo de criptografia**, o **algoritmo de autenticação** e os valores do **método das trocas de chave** devem combinar com os dados fornecidos no ASA.
9. Clique **em seguida** como mostrado aqui.
10. Nesta nova janela os detalhes **ajustados da transformação** devem ser fornecidos. O grupo da transformação especifica a **criptografia** e os **algoritmos de autenticação** usados para proteger **dados no VPN escavam um túnel**. Então, o clique **adiciona** para fornecer estes detalhes. Você pode adicionar todo o número de grupos Transform como necessário clicando **adicionar** e fornecendo os detalhes.
11. Forneça os detalhes **ajustados da transformação** (**criptografia e algoritmo de autenticação**) e clique a **APROVAÇÃO** como mostrado.
12. Escolha exigido **transformam o grupo** a ser usado para baixo da lista de gota como mostrado.
13. Clique em Next.
14. No seguinte indicador forneça os detalhes sobre o **tráfego a ser protegido** através do túnel VPN. Forneça a **fonte e as redes de destino do** tráfego a ser protegido de modo que o tráfego entre a fonte e as redes de destino especificadas seja protegido. Neste exemplo, a rede da fonte é 10.20.10.0 e a rede de destino é 10.10.10.0. Então, clique **em seguida**.
15. Este indicador mostra o sumário da configuração do VPN de Site-para-Site feita. Verifique a **conectividade de VPN do teste após ter configurado a** caixa de verificação se você quer testar a conectividade de VPN. Aqui, a caixa é verificada enquanto a Conectividade precisa de ser verificada. Então, **revestimento do** clique.
16. **Começo do** clique como mostrado para verificar a conectividade de VPN.
17. Na próxima janela que o resultado da **conectividade de VPN testa** é fornecido. Aqui, você

pode ver se o túnel é **para cima ou para baixo**. Neste exemplo de configuração, o túnel está **acima** segundo as indicações do verde.Isto termina a configuração no roteador do Cisco IOS.

Configuração do ASA via CLI

ASA

```
ASA#show run : Saved ASA Version 8.0(2) ! hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted names ! !---
Configure the outside interface. ! interface Ethernet0/1
nameif outside security-level 0 ip address 172.16.1.1
255.255.255.0 !--- Configure the inside interface. !
interface Ethernet0/2 nameif inside security-level 100
ip address 10.10.10.1 255.255.255.0 !-- Output
suppressed ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list 100 extended permit
ip any any access-list inside_nat0_outbound extended
permit ip 10.10.10.0 255.255.255.0 10.20.10.0
255.255.255.0 !--- This access list
(inside_nat0_outbound) is used !--- with the nat zero
command. This prevents traffic which !--- matches the
access list from undergoing network address translation
(NAT). !--- The traffic specified by this ACL is traffic
that is to be encrypted and !--- sent across the VPN
tunnel. This ACL is intentionally !--- the same as
(outside_1_cryptomap). !--- Two separate access lists
should always be used in this configuration. access-list
outside_1_cryptomap extended permit ip 10.10.10.0
255.255.255.0 10.20.10.0 255.255.255.0 !--- This access
list (outside_cryptomap) is used !--- with the crypto
map outside_map !--- to determine which traffic should
be encrypted and sent !--- across the tunnel. !--- This
ACL is intentionally the same as (inside_nat0_outbound).
!--- Two separate access lists should always be used in
this configuration. pager lines 24 mtu inside 1500 mtu
outside 1500 no failover asdm image disk0:/asdm-613.bin
asdm history enable arp timeout 14400 global (outside) 1
interface nat (inside) 1 10.10.10.0 255.255.255.0 nat
(inside) 0 access-list inside_nat0_outbound !--- NAT 0
prevents NAT for networks specified in !--- the ACL
inside_nat0_outbound. access-group 100 in interface
outside route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute http server enable http 0.0.0.0 0.0.0.0
dmz no snmp-server location no snmp-server contact !---
PHASE 2 CONFIGURATION ---! !--- The encryption types for
Phase 2 are defined here. crypto ipsec transform-set
ESP-DES-SHA esp-des esp-sha-hmac !--- Define the
transform set for Phase 2. crypto map outside_map 1
match address outside_1_cryptomap !--- Define which
traffic should be sent to the IPsec peer. crypto map
outside_map 1 set peer 172.17.1.1 !--- Sets the IPsec
peer crypto map outside_map 1 set transform-set ESP-DES-
SHA !--- Sets the IPsec transform set "ESP-AES-256-SHA"
!--- to be used with the crypto map entry "outside_map".
crypto map outside_map interface outside !--- Specifies
the interface to be used with !--- the settings defined
```

```
in this configuration. !--- PHASE 1 CONFIGURATION ---!
!--- This configuration uses isakmp policy 10. !--- The
configuration commands here define the Phase !--- 1
policy parameters that are used. crypto isakmp enable
outside crypto isakmp policy 10 authentication pre-share
encryption des hash sha group 1 lifetime 86400 telnet
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! tunnel-group 172.17.1.1 type ipsec-l2l !--
- In order to create and manage the database of
connection-specific !--- records for ipsec-l2l–IPsec
(LAN-to-LAN) tunnels, use the command !--- tunnel-group
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer. tunnel-group 172.17.1.1 ipsec-
attributes pre-shared-key * !--- Enter the pre-shared-
key in order to configure the !--- authentication
method. telnet timeout 5 ssh timeout 5 console timeout 0
threat-detection basic-threat threat-detection
statistics access-list ! class-map inspection_default
match default-inspection-traffic ! ! !-- Output
suppressed! username cisco123 password ffIRPGpDSOJh9YLq
encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end
```

Configuração de CLI do roteador

Router

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden as the default values are chosen.
```

```
crypto isakmp policy 2 authentication pre-share !---
Specifies the pre-shared key "cisco123" which should !--
- be identical at both peers. This is a global !---
configuration mode command. crypto isakmp key cisco123
address 172.16.1.1 ! ! !--- Configuration for IPsec
policies. !--- Enables the crypto transform
configuration mode, !--- where you can specify the
transform sets that are used !--- during an IPsec
negotiation. crypto ipsec transform-set ASA-IPSEC esp-
des esp-sha-hmac ! !--- !--- Indicates that IKE is used
to establish !--- the IPsec Security Association for
protecting the !--- traffic specified by this crypto map
entry. crypto map SDM_CMAP_1 1 ipsec-isakmp description
Tunnel to172.16.1.1 !--- !--- Sets the IP address of the
remote end. set peer 172.16.1.1 !--- !--- Configures
IPsec to use the transform-set !--- "ASA-IPSEC" defined
earlier in this configuration. set transform-set ASA-
IPSEC !--- !--- Specifies the interesting traffic to be
encrypted. match address 100 ! ! ! !--- Configures the
interface to use the !--- crypto map "SDM_CMAP_1" for
IPsec. interface FastEthernet0 ip address 172.17.1.1
255.255.255.0 duplex auto speed auto crypto map
SDM_CMAP_1 ! interface FastEthernet1 ip address
10.20.10.2 255.255.255.0 duplex auto speed auto !
interface FastEthernet2 no ip address ! interface Vlan1
ip address 10.77.241.109 255.255.255.192 ! ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2 ip route
10.77.233.0 255.255.255.0 10.77.241.65 ip route
172.16.1.0 255.255.255.0 172.17.1.2 ! ! ip nat inside
source route-map nonat interface FastEthernet0 overload
! ip http server ip http authentication local ip http
secure-server ! !--- Configure the access-lists and map
them to the Crypto map configured. access-list 100
remark SDM_ACL Category=4 access-list 100 remark IPSec
Rule access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255 ! ! ! !--- This ACL 110 identifies
the traffic flows using route map access-list 110 deny
ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255 access-list
110 permit ip 10.20.10.0 0.0.0.255 any route-map nonat
permit 10 match ip address 110 ! control-plane ! ! line
con 0 login local line aux 0 line vty 0 4 privilege
level 15 login local transport input telnet ssh ! end
```

Verificar

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

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

- Ferramenta de segurança PIX - comandos show
- IOS Router remoto - comandos show

Ferramenta de segurança ASA/PIX - comandos show

- **mostre isakmp cripto sa** — Mostra todo o IKE atual SA em um par.`ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 172.17.1.1 Type : L2L Role : initiator Rekey : no State : MM_ACTIVE`

- **mostre IPsec cripto sa** — Mostra todo o sas de IPSec atual em um par.`ASA#show crypto ipsec sa interface: outside Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1 local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) current_peer: 172.17.1.1 #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9 #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.1.1 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 434C4A7F inbound esp sas: spi: 0xB7C1948E (3082917006) transform: esp-des esp-sha-hmac none in use settings ={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0x434C4A7F (1129073279) transform: esp-des esp-sha-hmac none in use settings ={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y`

IOS Router remoto - comandos show

- **mostre isakmp cripto sa** — Mostra todo o IKE atual SA em um par.`Router#show crypto isakmp sa dst src state conn-id slot status 172.17.1.1 172.16.1.1 QM_IDLE 3 0 ACTIVE`
- **mostre IPsec cripto sa** — Mostra todo o sas de IPSec atual em um par.`Router#show crypto ipsec sa interface: FastEthernet0 Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1 protected vrf: (none) local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) current_peer 172.16.1.1 port 500 PERMIT, flags={origin_is_acl,} #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68 #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1 path mtu 1500, ip mtu 1500 current outbound spi: 0xB7C1948E(3082917006) inbound esp sas: spi: 0x434C4A7F(1129073279) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4578719/3004) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xB7C1948E(3082917006) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4578719/3002) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:`
- **active do show crypto engine connections** — Conexões atual e informação das mostras sobre pacotes criptografado e decriptografado (roteador somente).`Router#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt Decrypt 3 FastEthernet0 172.17.1.1 set HMAC_SHA+DES_56_CB 0 0 2001 FastEthernet0 172.17.1.1 set DES+SHA 0 59 2002 FastEthernet0 172.17.1.1 set DES+SHA 59 0`

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

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

Nota: Refira a informação importante em comandos Debug e em Troubleshooting de Segurança IP - compreendendo e usando comandos debug antes que você use **comandos debug**.

- **IPsec 7 do debug crypto** — Indica as negociações de IPSEC de fase 2.**isakmp 7 do debug crypto** — Indica as negociações de ISAKMP de fase 1.

- **IPsec do debug crypto** — Indica as negociações de IPSEC de fase 2.**isakmp do debug crypto** — Indica as negociações de ISAKMP de fase 1.

Refira a maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos soluções para obter mais informações sobre do Local-local VPN do Troubleshooting.

Informações Relacionadas

- Cisco PIX Firewall Software
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Profissional da configuração: IPSec local a local VPN entre ASA/PIX e um exemplo de configuração do IOS Router
- Referências do comando Cisco Secure PIX Firewall
- Cisco Router and Security Device Manager
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems