FORMAÇÃO EM CIBERSEGURANÇA

CISCO SECURE FIREWALL - VPN
(CERTIFICADO DIGITAL E PSK)

CIBERSEGURANCACISCO.COM.BR

JANEIRO/2025

DISCLAIMER

Esse material não tem qualquer relação oficial com a empresa CISCO. Ele foi criado por um profissional que trabalha há 20 anos com os equipamentos e soluções do fabricante.

A configuração mostrada não é uma recomendação. O autor não se responsabiliza por má utilização do material, que tem objetivo exclusivamente educativo (use-o para testar e aprender a ferramenta).

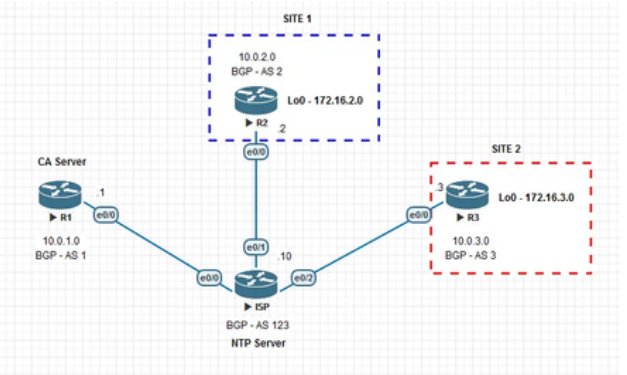
Esse ebook foi constituído a partir de artigos publicados de 2019 a 2021 no blog da TechRebels no medium.com pelo mesmo autor.

INTRODUÇÃO

Fala pessoal, tudo bem?

Hoje começaremos com o básico. Vamos brincar com VPN site-to-site autenticando com certificado digital e PSK. Usei roteadores, mas o conceito é exatamente o mesmo entre firewalls (seja ASA ou o Firepower), ok?

TOPOLOGIA



Topologia Site to Site IPSec com Certificado Digital

- **ISP** — Internet e NTP Server
- **R1** — CA Server
- **R2** — Site 1
- **R3** — Site 2

Obs: Para os estudos do CCIE acostumei a não usar mais rotas estáticas e sim um protocolo de roteamento dinâmico, sempre com autenticação. Isso consta no blueprint e cai na prova

R1

Após a conectividade estar ok a primeira coisa que fazemos é a geração da chave rsa

```
crypto key generate rsa label rsakey
```

Consulte a chave depois com o comando abaixo:

```
R1#sh crypto key mypubkey rsa
% Key pair was generated at: 11:27:31
BRT Oct 15 2019
Key name: rsakey
Key type: RSA KEYS
Storage Device: private-config
Usage: General Purpose Key
Key is not exportable.
```

Configuração da CA

Em seguida, vamos criar a CA Server. O método de enrollment que usaremos será via http, então precisamos habilitar o http server no router

```
R1#ip http server
crypto pki server ca-server
database level complete
no database archive
issuer-name CN=r1.lab.com
grant auto
```

O método de geração do certificado, que no nosso caso é automático (grant auto).

Caso fosse manual, após criar a requisição no R2 ou R3, teríamos que entrar com esse output na CA Server que irá gerar o certificado, copiá-lo e depois importá-lo no R2 ou R3. Então, pra facilitar (e como é um lab), podemos usar o modo automático.

O comando database level configura o nível de informações que será guardada na base de dados e o issuer-name o nome do host.

Feito isso, é só dar um ***no shutdown*** na CA Server

Para ver o status:

```
R1#sh crypto pki server
Certificate Server ca-server:

Status: enabled
State: enabled

Server's configuration is locked (enter
"shut" to unlock it)

Issuer name: CN=r1.lab.com

CA cert fingerprint: 090C3088 5F798668
32B78445 90C3080C

Granting mode is: auto

Last certificate issued serial number
(hex): 3
CA certificate expiration timer:
11:28:50 BRT Oct 14 2022
CRL NextUpdate timer: 17:28:17 BRT Oct
18 2019
Current primary storage dir: nvram:
Database Level: Complete — all issued
certs written as <serialnum>.cer
```

Caso a gente não habilite o ip http server, o status da CA Server estaria disabled.

R2 e R3

A config da CA está pronta, agora vamos criar um trustpoint em cada um dos sites.

Após criar a chave rsa utilizando o mesmo comando anterior — **crypto key generate rsa label rsakey** — vamos criar o trustpoint de nome *trustp-r2*

```
crypto pki trustpoint trustp-r2
enrollment url http://10.0.1.1:80
fqdn r3.lab.com
ip-address ethernet0/0
subject-name CN=r3.lab.com
revocation-check crl
rsakeypair rsakey
```

O enrollment url que apontamos para o R1, o fqdn e subject-name que será incluído no certificado, o nome da rsakey que criamos, e eu ainda gosto de adicionar o IP do router no certificado.

Finalizada a config, vamos autenticar o trustpoint e fazer o download do certificado do R1:

```
R2(config)#crypto pki authenticate trustp-r2
Certificate has the following attributes:
Fingerprint MD5: 090C3088 5F798668 32B78445 90C3080C
Fingerprint SHA1: 66F18FBC 68EE0171 25DEAFA3
A6A52B7F AD282B50
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

Por fim, vamos requisitar o nosso certificado para a CA Server, ou seja, vamos fazer o enrollment do R2

```
R2(config)#crypto pki enroll trustp-r2
%
% Start certificate enrollment ..
% Create a challenge password. You will need to
verbally provide this
password to the CA Administrator in order to revoke
your certificate.
For security reasons your password will not be saved
in the configuration.
Please make a note of it.
Password: xxxxxx
Re-enter password: xxxxxx
% The subject name in the certificate will include:
CN=r2.lab.com
% The subject name in the certificate will include:
r2.lab.com
% Include the router serial number in the subject
name? [yes/no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose trustp-
r2' command will show the fingerprint.
```

Após apenas alguns segundos, receberemos as mensagens abaixo

```
R2(config)#
*Oct 15 14:34:43.556: CRYPTO_PKI:
Certificate Request Fingerprint MD5:
27936625 CD9C0DC5 D3C7A746 03C2FDED
*Oct 15 14:34:43.557: CRYPTO_PKI:
Certificate Request Fingerprint SHA1:
1A927C3 1 5097B653 78FBEFC5 F19B8682
BD06CED7
R2(config)#
*Oct 15 14:34:43.613: %PKI-6-CERTRET:
Certificate received from Certificate
Authority
```

Temos agora o nosso certificado que será usado para autenticar a VPN site-to-site com o R3

Obs: Fazer o mesmo procedimento no R3

Para verificarmos o nosso certificado e o certificado da CA que baixamos:

```
R2#sh crypto pki certificates
Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer: cn=r1.lab.com
Subject: Name: r2.lab.com
IP Address: 10.0.2.2
ipaddress=10.0.2.2+hostname=r2.lab.com
cn=r2.lab.com
Validity Date:
start date: 11:34:43 BRT Oct 15 2019
end date: 11:34:43 BRT Oct 14 2020
Associated Trustpoints: trustp-r2
Storage: nvram:r1labcom#2.cer
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer: cn=r1.lab.com
Subject: cn=r1.lab.com
Validity Date:
start date: 11:28:50 BRT Oct 15 2019
end date: 11:28:50 BRT Oct 14 2022
Associated Trustpoints: trustp-r2
Storage: nvram:r1labcom#1CA.cer
```

VPN

Vamos agora pra configuração da VPN IPSec site-to-site:

Em primeiro lugar vamos definir o tráfego Interessante, ou o tráfego que será permitido passar pelo tunel

```
ip access-list extended VPN-R3
permit ip 172.16.2.0 0.0.0.255
172.16.3.0 0.0.0.255
```

Obs: Repare que é apenas o tráfego das loopbacks dos dois routers. Essas subnets simulam 2 servidores da rede LAN de cada site

```
crypto isakmp policy 10
authentication rsa-sig
encryption aes 256
hash sha256
group 2
```

O comando authentication rsa-sig vem por default e não aparece na config. Caso fôssemos usar pre-shared-key, teríamos que explicitar ***auth pre-shared-key***

```
crypto ipsec transform-set TSET esp-
3des esp-sha-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 10.0.3.3
set transform-set TSET
match address VPN-R3
reverse-route static
```

Habilitar a VPN na interface

```
interface Ethernet0/0
ip address 10.0.2.2 255.255.255.0
crypto map CMAP
```

Reparem que nós não temos rota para a loopback do R3 — afinal eu não publiquei ela no BGP e não adicionei nenhuma rota estática

```
R2#show ip route
10.0.0.0/8 is variably subnetted, 4
subnets, 2 masks
B 10.0.1.0/24 [20/0] via 10.0.2.10,
00:14:54
C 10.0.2.0/24 is directly connected,
Ethernet0/0
L 10.0.2.2/32 is directly connected,
Ethernet0/0
B 10.0.3.0/24 [20/0] via 10.0.2.10,
00:14:54
172.16.0.0/16 is variably subnetted, 3
subnets, 2 masks
C 172.16.2.0/24 is directly connected,
Loopback0
L 172.16.2.2/32 is directly connected,
Loopback0
R3#sh run | s router bgp
router bgp 3
bgp log-neighbor-changes
network 10.0.3.0 mask 255.255.255.0
neighbor 10.0.3.10 remote-as 123
neighbor 10.0.3.10 password cisco
```

A solução então é entrar com o comando destacado **reverse-route static**, que injeta uma rota estática baseado na nossa ACL de tráfego interessante

```
R2(config-crypto-map)#reverse-route ?
remote-peer Create route in route table
for remote tunnel endpoint
static Create routes based on static
ACLs permanently
```

VERIFICAÇÃO

Ping

```
R2#ping 172.16.3.3 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/7 ms
```

Fase 1

```
R2#sh crypto isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.0.2.2        10.0.3.3        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

```
R2#sh cry isa sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1003  10.0.2.2        10.0.3.3               ACTIVE aes  sha256 rsig 2  23:59:52
      Engine-id:Conn-id =  SW:3

IPv6 Crypto ISAKMP SA
```

Fase 2

```
R2#sh cry ipsec sa | i pkts
    #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: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
```

Alternando para pre-shared-key, teríamos essas mudanças na config

```
crypto isakmp policy 10
encr aes 256
hash sha256
authentication pre-share
group 2
crypto isakmp key cisco address 10.0.2.2
```

E após mudar o mesmo no R3, verificaríamos

```
R2#ping 172.16.3.3 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

```
R2#sh crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1002  10.0.2.2        10.0.3.3               ACTIVE aes  sha256 psk  2  23:55:43
      Engine-id:Conn-id =  SW:2

IPv6 Crypto ISAKMP SA
```

AGRADECIMENTOS

Gostaria de agradecer a todos os leitores e seguidores do blog TechRebels nesses anos todos. Foi sensacional ter tido a chance de conhecer alguns pessoalmente.

Espero que o conteúdo possa ajudar muito mais profissionais a melhorarem e crescerem profissionalmente.

Se você recebeu esse ebook de um amigo, dê uma olhada nos treinamentos que temos disponíveis no ciberseguranca cisco.com.br.

Grande abraço e muito sucesso!!!

linkedin.com/in/fmp7/