

IKEV2 TESTING

DAVIDE DE ZUANE & RAHMI EL MECHRI

CONTENTS

1 Introduction 3

1.1 IPsec 3

1.2 IKE 3

1.3 Strongswan 3

2 Setup 3

2.1 Environment 3

2.2 Configuration 3

3 Testing 4

3.1 Time 4

3.2 Performance 4

3.3 Results 4

4 Conslusioni 4

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

1 INTRODUCTION

L'aumento della connettività e n

La sicurezza negli ultimi anni sta diventando sempre più importante per le comunicazioni,

c'è sempre più bisogno di realizzare collegamenti sicuri, uno strumento molto utile a questo fine sono le VPN.

1.1 IPsec

IPsec (Internet Protocol Security) è una suite di protocolli che fornisce sicurezza alle comunicazioni Internet a livello IP. L'uso attuale più comune di IPsec è quello di fornire una rete privata virtuale (VPN). IKE (Internet Key Exchange) Internet Key Exchange) è il protocollo di negoziazione e gestione delle chiavi più comunemente munemente utilizzato per fornire chiavi negoziate e aggiornate dinamicamente per IPsec. Introduzione a quello che è ipsec e suo funzionamento

1.2 IKE

Importanza di IKE per effettuare lo scambio di chiavi per stabilire la SA.

Concetti su cui si basa IKE

1.3 Strongswan

Parlare rapidamente di quello che è quello che è anche l'architettura di strongswan charon.

2 SETUP

Descrivere come si è deciso di effettuare il testing. Vediamo anche quelle che sono le convenzioni che abbiamo utilizzato nella nostra sperimentazione.

2.1 Environment

<https://www.baeldung.com/linux/qemu-from-terminal>

Configurazione delle macchine virtuali utilizzate con KVM. quantità di ram e cpu assegnata, sistema operativo su cui si è effettuato il testing e in particolare la rete in modalità network bridge.

2.2 Configuration

```

/etc
├── ipsec.conf
├── ipsec.secret
├── ipsec.d
│   ├── cacerts
│   ├── certs
│   └── private

```

Certificati

IKEv2 supporta l'autenticazione tramite certificati, per poter avere dei certificati con delle firme valide occorre generare dei certificati da Root Authority. Per i test che andremo ad eseguire ci servono due certificati Root CA:

- un certificato RSA
- un certificato ECDSA

La caratteristica dei certificati Root CA è che sono autofirmati. Spiegare il perchè
Dunque procediamo con il generare la chiave privata della Root CA:

```
$ pki --gen --type rsa --size 2048 --outform pem > 'ca.rsa.key.pem'
$ pki --gen --type ecdsa --size 256 --outform pem > 'ca.ecdsa.key.pem'
```

Andiamo a creare i certificati di chiave pubblica andando ad applicare la chiave privata appena generata:

```
$ pki --self --ca --lifetime 3650 --in 'ca.<type>.key.pem' --type <type> --
dn "CN=Root_CA" --outform pem > ca.<type>.cert.pem
```

Generazione dei certificati, non si possono utilizzare i certificati presenti nel repository perchè sono legati all'IP del responder e dell'initiator.

```
$ pki --gen --type ecdsa --size 256 --outform pem > '/etc/ipsec.d/private'
```

2.2.1 Mschap

2.2.2 RSA

2.2.3 ECDSA

3 TESTING

Per misurare i cicli macchina abbiamo utilizzato perf

per installarlo apt-get install linux-perf se da problemi con workload failed è a causa dei permessi e per risolverlo basta sovrascrivere il contenuto di
/proc/sys/kernel/perf_event_paranoid per fare il report di tutto l'ambiente utilizzare perf report

3.1 Time

3.2 Performance

3.3 Results

4 CONSLUSIONI

REFERENCES