UNIVERSITÀ DEGLI STUDI ROMA TRE

Dipartimento di Ingegneria
Corso di Laurea in Ingegneria Informatica

Tesi Di Laurea

Realizzazione di un sistema di cyber-defense: utilizzo delle VPN per un accesso remoto sicuro a risorse interne

Laureando

Filippo Visconti

Matricola 547344

Relatore

Prof. Maurizio Patrignani

Anno Accademico 2021/2022

Questa è la dedica

Ringraziamenti

Questi sono i ringraziamenti.

Introduzione

Questa è l'introduzione.

Pericoli di esporre un server su internet

Prova di testo di capitolo.

Necessità di un'infrastruttura di rete sicura

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

Riassunto dei capitoli

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

Indice

Elenco delle figure

Capitolo 1

Requisiti

1.1 Caratteristiche della rete aziendale

Prova di testo di capitolo.

1.1.1 Diagramma di rete

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.1.2 Descrizione dei componenti fondamentali

1.1.2.1 Router/Firewall

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto. Ci gira CentOS 7 – che è quindi un requisito.

1.1.2.2 Le varie lan collegate

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.1.3 Servizi offerti all'esterno

Web servers, Database servers, File servers. Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.1.3.1 Web servers

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.1.3.2 Mail servers

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.1.3.3 Interfacce di controllo

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.1.4 Servizi offerti all'interno

1.1.4.1 DHCP

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.1.4.2 DNS

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.1.4.3 Web app interne

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.1.4.4 File servers

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.1.4.5 Database servers

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.2 Necessità degli utenti

1.2.1 Accessi ai servizi interni senza esposizione all'esterno

Router, Firewall, IDS, IPS, VPN. Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.2.1.1 Remote work

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.3 Requisiti di sicurezza

1.3.1 Controllo del traffico

1.3.1.1 Proxy interno obbligatorio

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.3.2 Trasmissione sicura dei dati

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.3.2.1 Evitare intercettazioni

Vedi Cina con il Great Firewall

1.3.3 Controllo dei dispositivi

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.3.3.1 Logs

Ancora del testo. Come si afferma in [JS96] molto lavoro deve ancora essere fatto.

1.3.4 Compatibilità

Deve essere compatibile con i 3 OS desktop e i 2 mobile principali

Capitolo 2

Stato dell'arte

2.1 Virtual Private Networks

2.1.1 Concetti fondamentali

Ancora del testo

2.1.2 Architetture disponibili

Ancora del testo

2.1.2.1 Gateway-to-Gateway

VPN gateway may be a dedicated de- vice or just a part of network device, such a router or firewall [11]. VPN 3 Background 11 gateway essentially separates internal network from anything over other side of gateway.

2.1.2.2 Host-to-Host

Primarily used to provide secure remote access. The host (IPsec client) uses VPN tunnel to connect to a VPN gateway. Whenever a host wishes to create a VPN connection to a server, he must authenticate and establish a connection with a gateway, which then manages host's connection to a VPN server.

2.1.2.3 Host-to-Gateway

Quella remote access

2.1.3 Soluzioni principali

PPTP, IPSec, OpenVPN, WireGuard.

2.1.4 Perché soddisfano i requisiti

Prova di testo di capitolo. Vorrei citare qui tutta l'opera omnia di [oEE90, Wik, Box97, AHPZ96].

2.2 IPSec

2.2.1 Panoramica

IPsec is a framework of open standards for ensuring private communications over IP networks which has become the most commonly used network layer security control [11]. IPsec is based on securing Network layer of TCP/IP model. In many environments securing Network layer is a better solution than securing higher Transport or Application layers. It makes a way for network administrators to enforce certain security policies, and also provides a more flexible way in protecting IP information for each packet [11]. Depending on the implementation IPsec can provide a combination of following security measures: confidentiality, integrity, peer authentication, replay protection, traffic analysis protection and access control

2.2.2 Protocolli utilizzati

Ancora del testo

2.2.2.1 Authentication Header

Ancora del testo

2.2.2.2 Encapsulating Security Payload

Ancora del testo

2.2.2.3 Internet Key Exchange v2

Ancora del testo—IKE è un acronimo per Internet key exchange ed è il protocollo usato per stabilire una security association nella suite di protocolli IPsec. Questo protocollo è definito in RFC 4306. È un protocollo di livello applicazione e utilizza il protocollo UDP come protocollo di trasporto; la porta su cui viene stabilita la connessione è 500. —

2.2.3 Transport mode vs Tunnel mode

Ancora del testo

2.2.4 Cifratura

Ancora del testo

2.2.5 Autenticazione

Ancora del testo

2.2.6 Implementazioni

StrongSwan is an open source IPsec implementation for the Linux oper- ating system [18]. Maintained by Andreas Steffen, strongSwan supports features, such as IPv6, Android 4+, X.509 public key certificates, certifi- cate revocation lists, RSA private key storage on smartcards, ability to interoperate with various MS Windows and Mac OS X VPN clients, full implementation of IKEv2 protocol, and much more.

2.2.7 Considerazioni

Ancora del testo

2.3 PPTP

2.3.1 Panoramica

Point-to-Point Tunneling Protocol (PPTP) is a virtual private network imple- mentation method which uses TCP control channel and a Generic Routing En- capsulation (GRE) tunnel to encapsulate Point-to-Point Protocol (PPP) [16] packets and send them over TCP/IP links. The protocol was developed by a vendor consortium and documented in RFC 2637 [17]. PPTP encapsulated virtual network packets inside the PPP packets, which are then encapsulated

3 Background 13 inside the GRE packets and these encapsulated inside the TCP control channel. Everything is then sent over IP network on TCP port 1723.

2.3.2 Protocolli utilizzati

Ancora del testo

2.3.2.1 Something

Ancora del testo

2.3.3 TCP vs UDP

Ancora del testo

2.3.4 Cifratura

NESSUNA

2.3.5 Autenticazione

Ancora del testo

2.3.6 Considerazioni

Ancora del testo

2.4 OpenVPN

2.4.1 Panoramica

OpenVPN is an SSL VPN implementation which implements OSI layer 2 or 3 secure network extension using the industry standard TLS proto- col [19].

2.4.2 Protocolli utilizzati

Ancora del testo

2.4.2.1 Something

Ancora del testo

2.4.3 TCP vs UDP

Ancora del testo

2.4.4 Cifratura

Ancora del testo

2.4.5 Autenticazione

Ancora del testo

2.4.6 Misure di sicurezza aggiuntive

Ancora del testo OpenVPN offers various internal security features. It has up to 256-bit encryption through the OpenSSL library, although some service providers may offer lower rates, effectively providing some of the fastest VPN available to consumers. It runs in userspace instead of requiring IP stack (therefore kernel) operation. OpenVPN has the ability to drop root privileges, use mlockall to prevent swapping sensitive data to disk, enter a chroot jail after initialization, and apply a SELinux context after initialization.

OpenVPN runs a custom security protocol based on SSL and TLS, rather than supporting IKE, IPsec, L2TP or PPTP.

OpenVPN offers support of smart cards via PKCS 11-based cryptographic tokens.

2.4.7 Considerazioni

Ancora del testo

2.5 WireGuard

2.5.1 Panoramica

Prova di testo di capitolo. Vorrei citare qui tutta l'opera omnia di [oEE90, Wik, Box97, AHPZ96].

2.5.2 Protocolli utilizzati

Ancora del testo

2.5.2.1 Something

Ancora del testo

2.5.3 TCP vs UDP

Ancora del testo

2.5.4 Cifratura

Ancora del testo

2.5.5 Autenticazione

Ancora del testo

2.5.6 Considerazioni

Ancora del testo

Capitolo 3

Realizzazione

3.1 Virtualizzatore

Ancora del testo

3.1.1 Caratteristiche e funzionamento

Ancora del testo

3.1.2 VirtualBox

Ancora del testo

3.1.3 VMWare ESXi

Ancora del testo

3.2 Installazione e configurazione dei servizi VPN

Ancora del testo

3.2.1 IPSec - tunnelmode

Ancora del testo

3.2.1.1 Installazione di stronSwan

Ancora del testo

3.2.1.2 Configurazione del Firewall

Ancora del testo

3.2.2 OpenVPN over TCP

Ancora del testo

3.2.2.1 Installazione di openvpn

Ancora del testo

3.2.2.2 Configurazione del Firewall

Ancora del testo

3.2.3 WireGuard

Ancora del testo

3.2.3.1 Installazione di wireguard

Ancora del testo

3.2.3.2 Configurazione del Firewall

Ancora del testo

Capitolo 4

Testing

4.1 Modalità di esecuzione dei test

Ancora del testo

4.1.1 Panoramica di iperf3

Ancora del testo

4.1.2 Scelta della configurazione di test

Ancora del testo

4.1.3 Criteri di valutazione

Ancora del testo

4.1.3.1 Throughput

Ancora del testo

4.1.3.2 MTU

Ancora del testo

4.1.3.3 Packetloss

Ancora del testo

4.2 Misure senza VPN

Ancora del testo

4.3 Misure con IPSec e IKEv2

Ancora del testo

4.4 Misure con OpenVPN over TCP

Ancora del testo

4.5 Misure con WireGuard

Ancora del testo

4.6 Analisi delle misure

Ancora del testo

Capitolo 5

Security concerns

5.1 Principali problematiche di sicurezza

Ancora del testo

5.2 Attacchi mirati agli utenti

Ancora del testo

5.3 Attacchi mirati al sistema

Ancora del testo

5.4 Multi-factor authentication

Ancora del testo

5.4.0.1 Certificato

Ancora del testo

5.4.0.2 Username e password

Ancora del testo

5.4.0.3 One Time Password

Ancora del testo

Conclusioni e sviluppi futuri

Quale è uscito vincitore

Ancora del testo

Come migliorare le misure

Ancora del testo

Test di VPN Peer-To-Peer

Ancora del testo

Zero Tier

Ancora del testo

Bibliografia

[AHPZ96] Eric Andonoff, Gilles Hubert, Annig Le Parc, and Gilles Zurfluh. Integrating versions in the omt models. In *ER '96: Proceedings of the 15th International Conference on Conceptual Modeling*, pages 472–487, London, UK, 1996. Springer-Verlag.

[Box97] D. Box. *Essential COM*. Addison Wesley Professional, 1997.

[JS96] Trevor H. Jones and Il-Yeol Song. Analysis of binary/ternary cardinality combinations in entity-relationship modeling. *Data Knowledge Engineering*, 19(1):39–64, 1996.

[oEE90] Institute of Electrical and Electronics Engineers. Ieee standard computer dictionary: A compilation of ieee standard computer glossaries, 1990.

[Wik] Wikipedia. `http://en.wikipedia.org/wiki/Interoperability`.