Titoli proposti:
Realizzazione di un sistema di cyber defence: studio e implementazione di un servizio VPN
Studio, implementazione e confronto di servizi VPN

1. Introduzione 2 pagine max scritta per ultima
    1. (Scopo del tirocinio)
    2. Pericoli di esporre un server su internet
    3. Necessità di un'infrastruttura di rete sicura
    4. 4-5 righe dove si spiega la tesi capitolo per capitolo
2. Requisiti
    1. Descrizione rete aziendale
    2. Diagramma configurazione di rete
        1. Diagramma e spiegazione
        2. Componenti fondamentali della rete
    3. Utente
        1. Accesso a servizi interni senza esposizione all'esterno
            1. Web server
            2. SSH
            3. FTP et similia
            4. Controllo sistemi
    4. Sistema
        1. Controllo e sicurezza del traffico tipo proxy interno obbligato
        2. Sicurezza nella trasmissione dei dati
            1. Assicurarsi che non ci siano intercettazioni
                1. Vd Cina col great Firewall
        3. Controllo dispositivi sia fissi che mobili
            1. Logs
    5. Servizi (in maniera sintetica)
        1. Server di dominio AD
        2. Mail server
        3. DNS
            1. Bind
        4. DHCP
            1. Dhcpd
        5. Proxy
            1. Squid
        6. Firewall
            1. iptables
            2. Forwarding
        7. IDS/IPS
            1. Snort
            2. FWSnort
            3. Crowdsec
        8. Web server
            1. httpd
            2. nginx come reverse proxy

6. Citare smartworking e utenti in mobilità (cellulare aziendale) come necessità, magari altre casistiche, vedi società di consulenza che hanno bisogno di accedere ai sistemi dei clienti senza magari essere presenti in loco
    1. Anche con diversi livelli e permessi di accesso (ad esempio a server specifici)
7. 3 OS desktop 2 mobile

3. Stato dell'arte (1/max 2 pagina ciascuno)
    1. Approfondimento su IPSec
        1. Come è nato
        2. Tipo incapsulamento
        3. Overhead - byte sprecati per pacchetto
        4. Livello a cui lavora
        5. Protocolli usati
        6. Cifratura usata ? hw o sw, limitata se non aggiorni hw ma più veloce, e il contrario
    2. Approfondimento su OpenVPN
        1. Come sopra
    3. Approfondimento su WireGuard
        1. Come sopra
4. Realizzazione
    1. Sistemi utilizzati
        1. Virtualizzatori
            1. Caratteristiche
            2. Applicativi usati
                1. Virtualbox
                2. VMWare ESXi
        2. OS
            1. CentOS 7
    2. Descrizione servizi VPN installati e scelte di configurazione
        1. IPSec (tunnel mode) - con strongSwan
        2. OpenVPN
        3. WireGuard
5. Testing prestazioni varie VPN
    1. Come viene eseguito il test
        1. Iperf3
        2. Installazione applicativi su server e client
    2. Criteri di valutazione
        1. Throughput
        2. MTU
        3. Packetloss
    3. Misure senza VPN
    4. Misure con IPSec
    5. Misure con OpenVPN
    6. Misure con WireGuard
    7. Analisi delle misure
6. Security concerns
    1. Ci possono essere numerosi problemi di sicurezza
        1. Attacchi mirati agli utenti
            1. Phishing
            2. Furto di credenziali

    2. Al sistema
        1. Versione non aggiornata
        2. Vulnerabilità note
            1. Sono tutti e tre open source, il che è la cosa migliore (e motivare perché)
            2. Amministratore di rete deve aggiornare tempestivamente il software al rilascio
            3. Potrebbero esistere non trovate
            4. Non solo nel codice, ma anche al progresso della tecnologia vd. computer quantistici che rompono alcune parti di cifratura
        3. Per mitigare questi problemi:
            1. Aggiornamenti
            2. MFA
2. Multi-factor authentication
    1. OTP
    2. Login
    3. Certificati
7. Conclusione e sviluppi futuri
    1. Riassunto della tesi
        1. Quale è il migliore e perché, oppure se non c'è il meglio
    2. Trovare un'idea per fare misure migliori
    3. Aggiungere test di VPN peer-to-peer come zerotier