SICUREZZA DELLE RETI

NUOVE TENDENZE [OBBLIGATORIE]

"NESSUNA RISORSA È INTRINSECAMENTE AFFIDABILE [ZERO TRUST]"

Autore: *Aldo Pedico* – Cybersecurity & Privacy
Contatto: pedicoaldo@gmail.com

Redatto il 7 agosto 2022

Per la scrittura di questo documento mi sono avvalso dei manuali: "NIST SP 800-207 – Zero Trust Architecture" e "NIST SP 800-215 – Guide to Secure Enterprise Network Landscape".
In particolare, ho tradotto e rielaborato il manuale "NIST SP 800-215"; dal "NIST SP 800-207" ho ripreso e sintetizzato alcuni concetti.

PERCHÉ HO REALIZZATO QUESTO DOCUMENTO

L'infrastruttura di un'azienda tipica è diventata sempre più complessa, gestendo diverse reti interne, uffici remoti con la propria infrastruttura locale, individui remoti e/o mobili e servizi cloud.

Questa complessità ***ha superato i metodi tradizionali di sicurezza*** *della rete basata sul perimetro* ***poiché non esiste un perimetro unico e facilmente identificabile per l'azienda****.*

Inoltre, la sicurezza della rete basata sul perimetro si è ***dimostrata insufficiente*** *poiché una volta che gli aggressori lo violano, non subiscono ostacoli per ulteriori movimenti trasversali [*EST-OVEST*].*

L'accesso a più servizi cloud, la diffusione geografica delle risorse IT aziendali (inclusi più data center) e l'emergere di applicazioni basate su microservizi hanno modificato in modo significativo il panorama delle reti aziendali.

Da non trascurare, è l'aumento dei dipendenti in telelavoro a causa della pandemia che ha reso necessario un mezzo per accedere alle risorse IT all'interno di una rete aziendale reti private virtuali (VPN).

In generale gli ambienti IT sono costituiti da: a) sottoscrizione a più servizi cloud, b) applicazioni IT aziendali (on-premise) distribuite, c) applicazioni IT sia monolitiche sia composte da microservizi ospitate su piattaforme eterogenee, e) presenza di dispositivi di edge computing.

Tali sistemi richiedono una connettività diffusa tra i sistemi IT e, a sua volta, comporta connettività:

- *tra risorse IT nei data center;*
- *tra risorse IT all'interno di una sede aziendale o di una filiale (Wi-Fi, LAN, VLAN);*
- *per gli utenti per accedere in remoto alle risorse IT da casa, luoghi di viaggio, filiali e uffici aziendali utilizzando WAN, che utilizzano più reti come Internet, MPLS e, in alcuni casi, reti cellulari (ad esempio, 4G / LTE, 5G, ecc.);*
- *ai servizi cloud tramite un provider di servizi cloud (CSP), networks private virtuali (VPN) o sottoscrizione a servizi WAN (licenze di apparecchiature locali o basate su cloud).*

*Per questo nuovo panorama di reti aziendali, questo documento ha lo scopo di fornire indicazioni da una prospettiva di "***OPERAZIONI SICURE***".*

Pertanto, inizia esaminando i limiti di sicurezza delle attuali soluzioni di accesso alla rete aziendale.

All'interno del documento, ho lasciato in evidenza i limiti dei presupposti e delle tecnologie di sicurezza dell'accesso alla rete esistenti a causa dei cambiamenti delle topologie di rete.

Sono inoltre discusse varie configurazioni di rete per l'autenticazione e l'autorizzazione di utenti, dispositivi e servizi, nonché la microsegmentazione per prevenire l'escalation degli attacchi.

Il documento esamina le più recenti tecnologie WAN che fanno parte dell'attuale panorama delle reti aziendali, nonché le caratteristiche delle offerte WAN con PoP globale e servizi di sicurezza integrati chiamati SASE.

QUALI SONO LE IMPLICAZIONI E I RISCHI

CONSIDERAZIONI

- *L'accesso ai servizi cloud da più provider cloud genera estensioni della rete aziendale; tale estensione, rientrando nell'ambito della gestione della rete aziendale, implica responsabilità e deve impedire che la sicurezza diventi una funzione critica.*
- *La distribuzione geografica delle risorse IT implica che gli utenti siano anch'essi distribuiti geograficamente.*

  Gli utenti possono ora accedere alle applicazioni dai locali aziendali, da filiali (attraverso la rete aziendale), ma anche da luoghi domestici e pubblici (ad esempio, hotel e bar) tramite dispositivi desktop, laptop e telefoni cellulari.

Garantire l'accesso sicuro da queste posizioni e dispositivi è responsabilità dell'azienda.

- *I cambiamenti nell'architettura delle applicazioni, passando a microservizi, aumentano i canali di comunicazione tra i componenti attraverso una rete ampliando la superficie di attacco a causa di:*
  a) *Architetture intrinseche;*
  b) *Strumenti di automazione;*
  c) *Metodologie di sviluppo e*
  d) *Distribuzioni.*

*DETERMINANO LE SEGUENTI **IMPLICAZIONI***

- SCOMPARSA DEL CONCETTO DI PERIMETRO DI RETE *che può essere protetto e della necessità di proteggere ogni endpoint (dispositivo o servizio) che lo tratta come un perimetro;*
- AUMENTO DELLA SUPERFICIE DI ATTACCO *grazie alla grande molteplicità di risorse IT (computing, networking, storage) e componenti;*
- AGGRESSORI PIÙ SOFISTICATI *nella loro capacità di intensificare gli attacchi attraverso diversi confini di rete e sfruttare le funzionalità di connettività.*

ALCUNI RISCHI (nei capitoli successivi maggiori dettagli)

- *Aumento della latenza di rete e potenziali colli di bottiglia del traffico per effetto dei percorsi aggiuntivi delle connessioni VPN stabilite dagli utenti remoti che terminano nei relativi concentratori situati ai margini della rete aziendale.*
- *Compromissione dei dispositivi ed entrata "in casa" con conseguenti attacchi di phishing.*
- "DIROTTAMENTO DELLA SESSIONE" *(Session Hijacking).*
- *Accesso non autenticato alla console di amministrazione VPN tramite Pulling di un ID univoco.*

QUALI AZIONI CORRETTIVE INTRAPRENDERE

Da quanto detto in precedenza, è evidente che scompaiono sia il perimetro di rete sia la distribuzione dei target applicativi (essendo un ambiente applicativo ibrido); a questo punto le aziende

*dovrebbero adottare un paradigma "*ENDPOINT È IL PERIMETRO*" e disporre di un sistema di gestione dei dispositivi.*

Qui ci viene incontro ZERO TRUST (ZT).

ZT è un insieme in evoluzione di paradigmi di sicurezza informatica che spostano le difese da perimetri statici basati sulla rete (poiché il percorso di rete non è più visto come il componente principale della posizione di sicurezza della risorsa) per concentrarsi su utenti, beni e risorse.

ZT presuppone che non vi sia alcun trust (garanzia scontata!) implicito concesso alle risorse o agli account utente in base esclusivamente al loro percorso fisico o di rete (ad esempio, reti locali rispetto a Internet) o in base alla proprietà delle risorse (aziendale o di proprietà personale).

Per spostare maggiormente l'attenzione sulle risorse, si adotta la tecnica SEGMENTAZIONE.

Tale tecnica presenta i seguenti vantaggi:

a) *i segmenti isolati e relativamente piccoli consentono un attento monitoraggio del traffico grazie a una migliore visibilità;*
b) *l'abilitazione delle funzionalità limita il movimento laterale (*EST-OVEST*) non autorizzato.*

Il motivo per cui la microsegmentazione basata sull'identità è studiata nel panorama delle reti aziendali è che ***consente solo un traffico di rete valido tra i vari servizi componenti dell'applicazione*** *a causa dell'autenticazione e dell'autorizzazione reciproche utilizzando le identità del servizio, consentendo così di raggiungere gli obiettivi dell'accesso alla rete* ZERO TRUST (ZTNA).

INDICE DEGLI ARGOMENTI

Titolo _____ Pag.

1 - INTRODUZIONE

La rete WAN (WIDE AREA NETWORK) *è diventata parte integrante della rete aziendale quando le organizzazioni hanno avuto bisogno di connettere le loro reti locali* (LAN) *su più posizioni geograficamente distribuite (all'interno del paese e, in alcuni casi, a livello globale) a partire dal 1980.*

La tecnologia WAN iniziale prevedeva linee affittate POINT-TO-POINT (P2P) *seguite da* FRAME RELAY.

*La prima rete basata su IP era la commutazione di etichette multiprotocollo (*MULTI PROTOCOL LABEL SWITCHING - MPLS*), che consentiva a più tipi di traffico, come voce, video e dati, di viaggiare sulla stessa linea.*

Con l'avvento di tecnologie come la virtualizzazione e l'aumento dell'accesso aziendale ai servizi cloud, le aziende hanno iniziato ad adottare una nuova tecnologia WAN (WIDE AREA NETWORK) *chiamata* SOFTWARE-DEFINED WAN (SD-WAN).

La tecnologia SD-WAN *rimuove lo stretto accoppiamento tra il piano di controllo e le funzioni del piano dati della rete, consentendo la precisazione centralizzata di vari criteri, come il controllo degli accessi, il routing e la prioritizzazione del traffico delle applicazioni.*

Un altro sviluppo ha riguardato l'integrazione di tutte le soluzioni di sicurezza puntuale fornite da varie apparati di sicurezza di rete in un'infrastruttura di servizi di sicurezza di rete.

L'accesso a più servizi cloud, la diffusione geografica delle risorse IT aziendali (inclusi più data center) e l'emergere di applicazioni basate su microservizi (al contrario di quelle monolitiche) hanno modificato in modo significativo il panorama delle reti aziendali.

Questo documento ha lo scopo di fornire indicazioni per questo nuovo panorama di reti aziendali da una prospettiva di operazioni sicure.

Pertanto, inizia esaminando i limiti di sicurezza delle attuali soluzioni di accesso alla rete alla rete aziendale e successivamente considera:

a) *i miglioramenti delle funzionalità di sicurezza dei dispositivi di rete tradizionali sotto forma di soluzioni di sicurezza puntuale,*

b) *configurazioni di rete per varie funzioni di sicurezza (ad esempio, sicurezza delle applicazioni, sicurezza dell'accesso al cloud, sicurezza dei dispositivi o degli endpoint, ecc.),*

c) *Framework di sicurezza che integrano queste singole configurazioni di rete e*

d) *l'infrastruttura WAN (Wide Area Network) in evoluzione per fornire un set completo di servizi di sicurezza per il moderno panorama di rete aziendale.*

Nell'ultimo decennio, il panorama delle reti aziendali ha subito enormi cambiamenti a causa dei seguenti tre driver:

1. *Accesso aziendale a più servizi cloud,*
2. *La diffusione geografica delle risorse IT aziendali (on-premise) (ad esempio, più data center e filiali),*

3. *Modifiche all'architettura dell'applicazione da monolitiche a un set di microservizi ad accoppiamento debole, spesso con un'infrastruttura dedicata (chiamata* SERVICE MESH*) che fornisce tutti i servizi applicativi, compresa la sicurezza.*

L'impatto di questi driver sulla sicurezza del panorama delle reti aziendali include:

1. *Scomparsa del concetto di perimetro di rete che può essere protetto e della necessità di proteggere ogni endpoint (dispositivo o servizio) che lo tratta come un perimetro;*
2. *Aumento della superficie di attacco grazie alla grande molteplicità di risorse IT (computing, networking, storage) e componenti;*
3. *Sofisticazione degli aggressori nella loro capacità di intensificare gli attacchi attraverso diversi confini di rete e sfruttare le funzionalità di connettività.*

Questo documento ha lo scopo di fornire indicazioni per questo nuovo panorama di reti aziendali da una prospettiva di operazioni sicure.

La metodologia adottata considera le sfide di sicurezza che la rete pone e quindi esamina i limiti delle attuali tecnologie di accesso alla rete e il modo in cui le soluzioni si sono evolute dall'essere specifiche della funzione di sicurezza a un framework di sicurezza a un'infrastruttura di sicurezza completa che fornisce un insieme olistico di servizi di sicurezza.

Le aree specifiche affrontate includono:

1. *Miglioramenti delle funzionalità degli apparati di sicurezza di rete tradizionali;*
2. *Protezione delle configurazioni di rete aziendali per vari scenari;*
3. *Framework di sicurezza che integrano singole configurazioni di rete;*
4. *Infrastruttura* WAN (WIDE AREA NETWORK) *in evoluzione che fornisce un set completo di servizi di sicurezza.*

Quella che viene definita come la rete aziendale in questo documento comprende le varie reti locali nei locali aziendali e quella parte della rete WAN che viene utilizzata per connettere le sue varie posizioni geograficamente disperse e i punti di accesso ai servizi cloud.

1.1 - IMPLICAZIONI STRUTTURALI DEI DRIVER NEL PANORAMA DELLE RETI AZIENDALI

Per avere una buona visione strutturale dell'attuale panorama delle reti aziendali, è necessario guardare all'attuale ambiente IT aziendale in generale.

L'ambiente IT è ora costituito da:

1. *Sottoscrizione a più servizi cloud, come* **IaaS *per l'elaborazione,* SaaS *per il software,* PaaS *per una piattaforma di sviluppo di applicazioni e altri servizi cloud (ad esempio,* IDaaS *per l'autenticazione***);**

2. *Applicazioni IT aziendali (on-premise) situate nella sede centrale dell'azienda e nelle filiali e nei data center geograficamente distribuiti;*
3. *Le applicazioni IT vanno dall'essere monolitiche a quelle costituite da microservizi ad accoppiamento debole, ognuno dei quali ospitato su piattaforme eterogenee;*
4. *Presenza di dispositivi di edge computing, come gli IoT, in alcuni ambienti.*

Gli scenari di cui sopra richiedono una connettività diffusa tra i sistemi IT che ora definisce l'attuale panorama delle reti aziendali.

La connettività, a sua volta, comporta:

1. *Connettività tra risorse IT (server per l'elaborazione e lo storage) nei data center (infrastruttura di rete);*
2. *Connettività tra risorse IT all'interno di una sede aziendale o di una filiale (Wi-Fi, LAN, VLAN);*
3. *Connettività per gli utenti per accedere in remoto alle risorse IT da casa, luoghi di viaggio, filiali e uffici aziendali utilizzando WAN, che utilizzano più reti come Internet, MPLS e, in alcuni casi, reti cellulari (ad esempio, 4G / LTE, 5G, ecc.);*
4. *Connettività ai servizi cloud tramite un provider di servizi cloud (CSP), networks private virtuali (VPN) o sottoscrizione a servizi WAN (licenze di apparecchiature locali o basate su cloud).*

1.2 - IMPLICAZIONI PER LA SICUREZZA DEI DRIVER PER IL PANORAMA DELLE RETI AZIENDALI

All'inizio di questa sezione sono indicati i seguenti driver per lo stato del panorama di rete aziendale corrente:

1. SOTTOSCRIZIONE A PIÙ SERVIZI CLOUD;
2. RISORSE IT DISTRIBUITE GEOGRAFICAMENTE;
3. MODIFICHE NELL'ARCHITETTURA DELL'APPLICAZIONE;

IMPLICAZIONI IMMEDIATE PER LA SICUREZZA DEI SUDDETTI DRIVER

1. SOTTOSCRIZIONE A PIÙ SERVIZI CLOUD

L'accesso ai servizi cloud da più provider cloud è diventato la norma per molte aziende.

Questa tendenza è motivata non solo dalla necessità di evitare una situazione di LOCK-IN (*si verifica quando il passaggio da un fornitore cloud ad un altro è difficile e costosa, rendendo i clienti*

più dipendenti - bloccati/look*) del fornitore di cloud, ma anche da diversi CSP che offrono diverse funzioni a valore aggiunto per diversi servizi (ad esempio, IaaS, SaaS).*

La conseguenza di questa tendenza è che *– da un punto di vista aziendale –* le seguenti reti sono diventate estensioni della propria rete e, come tali, rientrano nell'ambito della gestione della propria rete implicando responsabilità: deve essere impedito che la sicurezza diventi una funzione critica.

a) *Rete utilizzata per l'accesso ai servizi cloud.*

b) *Rete inter-cloud (poiché la comunicazione tra un CSP e l'altro può essere inevitabile).*

c) *La rete all'interno del provider cloud che deve essere navigata per accedere ai servizi sottoscritti (ad esempio, VPC, VNET, ecc.).*

2. RISORSE IT DISTRIBUITE GEOGRAFICAMENTE

L'implicazione delle risorse IT distribuite è che gli utenti sono anche distribuiti geograficamente.

Gli utenti possono ora accedere alle applicazioni non solo dai locali aziendali, come l'ufficio aziendale e le filiali (attraverso la rete aziendale), ma anche da luoghi domestici e pubblici (ad esempio, hotel e bar) tramite più dispositivi, come desktop, laptop e telefoni cellulari.

Garantire l'accesso sicuro da queste più posizioni e dispositivi diventa responsabilità dell'azienda.

3. CAMBIAMENTI NELL'ARCHITETTURA DELLE APPLICAZIONI

Le architetture delle applicazioni, in particolare quelle delle applicazioni native del cloud, sono passate dall'essere monolitiche ad essere basate su microservizi, con la natura distribuita che aumenta i canali di comunicazione tra i componenti attraverso una rete (invece di essere solo chiamate di procedura/funzione locali*).*

Queste applicazioni hanno ampliato la superficie di minaccia e attacco a causa di:

a) *Architetture intrinseche (più microservizi e API indipendenti),*

b) *Strumenti di automazione utilizzati durante lo sviluppo e la distribuzione del software e*

c) *Metodologie di sviluppo e distribuzione agili, ad esempio DevSecOps, che contengono codice pipeline CI/CD (flussi di lavoro).*

Gli attacchi includono violazioni dei dati, DDOS (DISTRIBUTED DENIAL OF SERVICE)*, acquisizione di account* (ACCOUNT TAKEOVER *-* ATO*) a causa del furto di credenziali e minacce interne.*

1.3 - NECESSITÀ DI UNA GUIDA ALLA SICUREZZA

Sulla base delle suddette considerazioni per l'implementazione della sicurezza, gli argomenti a favore della necessità di una GUIDA ALLA SICUREZZA *per l'attuale panorama delle reti aziendali sono:*

1. Le posizioni di accesso onnipresenti, le posizioni di hosting onnipresenti dei componenti dell'applicazione e i protocolli di trasporto WAN multipli hanno causato cambiamenti nei focus, negli obiettivi e nei principi di sicurezza.
2. L'attenzione alla sicurezza si è ampliata dall'essere incentrata sulla rete (ad esempio, rete interna / aziendale rispetto a Internet esterna / pubblica) a incentrata sull'utente e sul dispositivo / endpoint.
3. La nuova relazione di trust deve essere basata non solo sull'identità o sulla posizione dell'accesso, ma deve essere migliorata per includere la convalida di ogni richiesta di accesso (non solo all'inizio di una sessione di accesso), nonché l'insieme applicabile di informazioni contestuali associate all'utente, al dispositivo o al servizio.

2. - APPROCCI TRADIZIONALI ALL'ACCESSO ALLA RETE AZIENDALE E LORO LIMITI

Entrambi i driver (**cambiamento nelle architetture delle applicazioni e accesso alle applicazioni basate su cloud**) *hanno avuto un impatto sui meccanismi di accesso sicuro a tali applicazioni attraverso la rete.*

Consideriamo ora i limiti di sicurezza dei tradizionali approcci di accesso alla rete aziendale nell'attuale contesto del panorama della rete aziendale.

1. LIMITAZIONE DELLE PROTEZIONI BASATE SUL PERIMETRO DI RETE.
2. LIMITAZIONI DELL'ACCESSO BASATO SU VPN.
3. LIMITAZIONI DELLA TECNOLOGIA MPLS COME WAN AZIENDALI.
4. LIMITAZIONE DEI CONTROLLI BASATI SULL'IDENTITÀ DELL'UTENTE.

2.1 - LIMITAZIONI DELLE PROTEZIONI BASATE SUL PERIMETRO DI RETE

Le prime soluzioni per l'accesso sicuro alla rete aziendale erano orientate verso ambienti con perimetri di rete ben definiti.

Tutte le risorse IT aziendali erano endpoint di LAN (di solito definite come un piano in una grande impresa, edificio o piccolo campus) e più LAN collegate tra loro all'interno di un edificio o campus definito costituivano la rete aziendale interna.

I punti di ingresso in questa rete aziendale sono stati protetti utilizzando dispositivi chiamati firewall, che sono stati inizialmente implementati come dispositivi hw e successivamente sw.

In questo ambiente, tutti i dispositivi e gli utenti all'interno dei firewall erano totalmente affidabili e, quindi, considerati sicuri per l'accesso alle risorse dell'applicazione.

Tuttavia, i seguenti elementi hanno **annullato la nozione di tale perimetro:**

1. Natura distribuita dell'applicazione in quelle situate all'interno di un data center aziendale, filiali remote e più sedi cloud.
2. Approccio perimetrale basato sulla premessa che la minaccia ha origine al di fuori della rete, motivo per cui la maggior parte delle soluzioni di sicurezza perimetrale (ad esempio, IPS, IDS, firewall) si concentrano solo sul traffico **NORD-SUD**. Tuttavia, oltre il 75% del traffico di rete è ora **EST-OVEST** o **SERVER-TO SERVER** (a causa delle applicazioni basate su microservizi), il che è in gran parte invisibile ai team di sicurezza. Qualsiasi minaccia che si trova già all'interno di una rete può spostarsi lateralmente e rimanere inosservata per giorni o addirittura mesi.
3. EDGE COMPUTING, in cui gran parte dell'elaborazione avviene vicino alla posizione di più dispositivi IoT.
4. Utenti che si trovano sia all'interno che all'esterno della rete aziendale, ad esempio in case, filiali remote e luoghi pubblici (ad esempio, hotel, pub, ecc.). Alcune aziende devono anche fornire l'accesso ai partner dell'ecosistema, che possono trovarsi sulle proprie reti aziendali.

GLI SCENARI DI CUI SOPRA HANNO NOTEVOLMENTE AMPLIATO LA SUPERFICIE DI ATTACCO.

2.2 - RISCHI CON ACCESSO BASATO SU VPN

L'aumento dei dipendenti in telelavoro a causa della pandemia ha reso necessario un mezzo per un accesso sicuro alle risorse IT all'interno di una rete aziendale sotto forma di reti private virtuali (VPN)*.*

La VPN consente alle organizzazioni di estendere una sicurezza basata sul perimetro su una rete pubblica.

La sicurezza è abilitata impostando un tunnel sicuro nella rete pubblica utilizzando protocolli come IPSEC *e* TLS.

Tuttavia, ci sono alcune limitazioni e, di conseguenza, rischi per la sicurezza associati alle VPN.

1. La tendenza crescente prevede lo spostamento delle risorse aziendali verso il cloud e l'utilizzo di dispositivi mobili.

   Le connessioni VPN stabilite dagli utenti remoti terminano nei concentratori VPN situati ai margini della rete aziendale.

   Quindi, utilizzando un processo chiamato HAIR PINNING, il traffico che atterra al bordo Internet aziendale viene reindirizzato a Internet per accedere alle risorse cloud. Questo percorso aggiuntivo aumenta la latenza di rete e ha il potenziale di causare colli di bottiglia del traffico.

2. I dispositivi mobili utilizzati da molti dipendenti, come smartphone e tablet, possono connettersi direttamente alle applicazioni SOFTWARE-AS-A-SERVICE (SAAS) e ai dati nel cloud.

   Questi dispositivi mobili sono particolarmente soggetti ad attacchi di phishing che rubano credenziali o forniscono malware.

   Pertanto, la VPN diventa un punto di ingresso attraverso il quale un malintenzionato potrebbe compromettere un dispositivo ed entrare nell'infrastruttura di un'organizzazione.

3. Due recenti vulnerabilità sono state scoperte in alcune VPN.

   La prima era il "**dirottamento della sessione**" **(Session Hijacking)**, in cui attori malintenzionati accedono a un ID di sessione valido tramite attacchi di forza bruta o reverse engineering.

   La seconda riguardava il **PULLING** di un ID univoco per un account, l'utilizzo di strumenti di sviluppo del browser Web per impostare manualmente un valore sull'ID e l'utilizzo di tale valore per ottenere l'accesso non autenticato alla console di amministrazione VPN.

   Tale accesso è stato quindi utilizzato per connettersi in remoto ai sistemi interni, raccogliere password, spostarsi lateralmente nella rete e, in molti casi, distribuire ransomware.

2.3 - LIMITAZIONE DELLA TECNOLOGIA MPLS COME WAN AZIENDALI

La tecnologia MPLS (MULTI-PROTOCOL LABEL SWITCHING) *è utilizzata per le WAN aziendali, ma l'ampia estensione geografica di una rete aziendale a causa di più data center e servizi cloud ha imposto alcune limitazioni al suo utilizzo.*

1. *L'estensione geografica delle risorse IT aziendali e le successive connessioni di rete hanno reso inevitabile l'attraversamento di Internet per molte parti della rete di accesso della propria azienda. Poiché MPLS è una rete diversa, fornisce l'accesso a Internet solo attraverso punti di accesso designati e limitati. Ciò aumenta la latenza per le applicazioni aziendali sensibili al fattore tempo.*
2. *Data la diversa tecnologia di rete, le apparati e le successive procedure di configurazione sono diverse, rendendo la gestione della rete un compito complesso.*

2.4 - LIMITAZIONE (RISCHI) DEI CONTROLLI BASATI SU IDENTITÀ UTENTE

Nelle applicazioni monolitiche tradizionali, tutte le richieste di applicazioni provengono direttamente dall'utente o tramite script scritti e sono da esso programmati per l'esecuzione.

Pertanto, gli unici parametri per la convalida dell'accesso sono l'identità dell'utente o gli attributi associati all'utente.

Le modifiche apportate alle architetture espandono i parametri di convalida oltre l'identità e gli attributi dell'utente. Tali modifiche si trovano nelle applicazioni basate sia sul Web sia su API in cui l'accesso può avvenire da qualsiasi dispositivo situato in qualsiasi rete (ad esempio, casa, WiFi pubblico, ecc.).

Le ultime modifiche si trovano nelle applicazioni basate su microservizi (spesso chiamate applicazioni native del cloud perché questa architettura è quella predominante tra le applicazioni ospitate nel cloud).

Questa classe di applicazioni è costituita da microservizi ad accoppiamento debole *che richiede la generazione di più richieste interservizi per completare un processo o una transazione.*

Le limitazioni dei controlli basati sull'identità sono visibili dai seguenti requisiti di sicurezza estesi per le applicazioni basate su microservizi:

1. *La validazione è richiesta non solo per l'identità degli utenti che avviano la transazione ma anche per l'identità di ciascun servizio* (identità del servizio) *che effettua la richiesta e del dispositivo su cui è ospitato il servizio* (dispositivo autorizzato).
2. *La posizione del servizio e del dispositivo può cambiare a causa della natura virtualizzata dell'ambiente di hosting dell'applicazione (ad esempio, migrazione a macchine virtuali situate in una sottorete diversa, dispositivi di hosting e meccanismi di archiviazione più potenti, ecc.), rendendo necessaria la convalida di una richiesta di applicazione* basata non solo sull'identità e sugli attributi dell'utente, *ma* anche sugli attributi associati al dispositivo, *rete, geolocalizzazione, ecc.*
3. La convalida dell'identità (autenticazione) e dell'autorizzazione deve essere eseguita continuamente *(e non solo all'inizio di una sessione di invocazione dell'applicazione) poiché il profilo di rischio di un accesso può cambiare a causa della presenza di più entità coinvolte o*

di cambiamenti nei modelli comportamentali che devono essere inclusi come parametro di convalida (e monitorati).

3 - DISPOSITIVI DI SICUREZZA DI RETE NEL PANORAMA DELLE RETI AZIENDALI

Questa sezione prenderà in considerazione alcuni nuovi dispositivi di sicurezza di rete e funzionalità avanzate in apparecchiature consolidate per soddisfare le esigenze di sicurezza del panorama attuale.

3.1 - CLOUD ACCESS SECURITY BROKER (CASB)

Data la crescente sottoscrizione a più cloud, uno dei software più importanti è il CLOUD ACCESS SECURITY BROKER (CASB).

Proprio come i sistemi IAM, un CASB può essere eseguito in locale o come servizio basato su cloud.

*Si trova sulla rete tra i clienti del servizio cloud (*CLOUD SERVICE CUSTOMER - CSC*) e i provider di servizi cloud (*CLOUD SERVICE PROVIDER - CSP*).*

L'evoluzione della funzionalità CASB può essere tracciata come segue:

1. *La funzione primaria della prima generazione di CASB era la scoperta delle risorse.*

   Hanno fornito visibilità su tutte le risorse cloud a cui gli utenti aziendali hanno avuto accesso, prevenendo o riducendo al minimo le possibilità di shadow IT.

   Un esempio di questo è l'uso di applicazioni SOFTWARE-AS-A-SERVICE (SAAS) *non approvate per la condivisione di file, i social media, la collaborazione e le conferenze Web da parte di alcuni utenti aziendali.*

   Questa generazione di CASB fornisce anche alcune statistiche, come l'utilizzo del SOFTWARE-AS-A-SERVICE (SaaS).

2. *L'attuale generazione di CASB applica policy di sicurezza e governance per le applicazioni cloud, consentendo così alle aziende di estendere le proprie policy on-premise al cloud.*

   I servizi di sicurezza specifici forniti dai CASB includono:

   a. PROTEZIONE DEI DATI AZIENDALI *che risiedono nei server dei provider di servizi cloud (SAAS o IAAS), nonché afflusso e deflusso di dati da tali server;*

   b. MONITORAGGIO DELLE MINACCE, *come il dirottamento dell'account e altre attività dannose.*

      Alcuni possono rilevare anomalie nel comportamento di accesso al cloud degli utenti (attraverso solide funzionalità di analisi del comportamento di utenti ed entità o USER

AND ENTITY BEHAVIOR ANALYTICS - UEBA*) e bloccare le minacce interne e gli attacchi informatici avanzati.*

c. RILEVAMENTO DI CONFIGURAZIONI ERRATE *nell'infrastruttura subscribed* INFRASTRUCTURE AS A SERVICE (IAAS) *e nei server cloud dell'azienda.*

   Queste configurazioni errate comportano gravi rischi per la sicurezza, come le violazioni dei dati.

   Gli avvisi generati da CASB a causa di configurazioni errate nelle distribuzioni IaaS dell'azienda indirizzano l'azienda a seguire linee guida, come i benchmark del CENTER FOR INTERNET SECURITY (CIS) *per i servizi cloud pubblici, migliorando così il profilo di sicurezza generale dell'azienda per l'accesso al cloud.*

3.2 - FUNZIONALITÀ FIREWALL AVANZATE

I firewall sono nati come apparati hardware che impedivano ai pacchetti di rete di un dispositivo con un particolare percorso di rete (ad esempio, combinazione di indirizzo IP e porta) in una subnet (ad esempio, rete esterna o Internet) di accedere a un dispositivo su un altro percorso di rete o subnet (ad esempio, intranet o DMZ o rete aziendale).

In tale configurazione, ha protetto principalmente un perimetro di rete.

L'evoluzione delle funzioni firewall può essere tracciata in base ai seguenti set di funzionalità:

1. FILTRI DEI PACCHETTI E TRADUZIONE DEGLI INDIRIZZI DI RETE (NETWORK ADDRESS TRANSLATION – NAT): *il filtraggio dei pacchetti e NAT sono utilizzati per:*
   a. *monitorare e controllare i pacchetti che si spostano su un'interfaccia di rete,*
   b. *applicare regole di sicurezza predeterminate e*
   c. *oscurare la rete interna dalla rete Internet pubblica.*
2. ISPEZIONE STATEFUL: *il firewall stateful, noto anche come filtraggio dinamico dei pacchetti, monitora lo stato delle connessioni e determina quali tipi di pacchetti di dati appartenenti a una connessione attiva nota possono passare attraverso il firewall.*
3. RILEVAMENTO E RISPOSTA ALLE MINACCE: *i firewall attuali possono raccogliere e analizzare dati sufficienti su più pacchetti e sessioni per rilevare minacce e incidenti di sicurezza mirati a un particolare sistema o a una famiglia di sistemi.*

   I dati provenienti da più firewall possono anche essere indirizzati verso la gestione delle informazioni e degli eventi di sicurezza (SECURITY INFORMATION AND EVENT

MANAGEMENT -SIEM*) e correlati con i dati provenienti da altri strumenti di sicurezza e sistemi IT per rilevare attacchi a livello aziendale che si estendono su più sistemi e livelli di rete.*

4. FUNZIONALITÀ DI REGISTRAZIONE E CONTROLLO*: le funzionalità di registrazione e controllo comportano la creazione di eventi di rete che possono essere utilizzati per identificare modelli di problemi di prestazioni e sicurezza.*

5. FUNZIONI DI CONTROLLO DEGLI ACCESSI*: le funzioni di controllo degli accessi applicano criteri di controllo degli accessi granulari e sofisticati.*

6. POSIZIONI E FUNZIONI MULTIPLE*: i firewall risiedono in posizioni diverse per eseguire funzioni diverse.*

   *I firewall all'*Edge *della rete eseguono la funzione di protezione perimetrale della rete filtrando le origini e le destinazioni non consentite e bloccando i pacchetti di potenziali minacce.*

   I firewall all'interno di un data center possono creare segmentazione della rete interna per impedire il movimento laterale (EST-OVEST) del traffico e isolare le risorse sensibili *(ad esempio, servizi e archivi dati).*

   I firewall basati su dispositivo impediscono il traffico dannoso in entrata e in uscita dagli endpoint.

7. *Le API aperte si integrano con molti prodotti di rete.*

8. *Alcune funzionalità definiscono o uniscono centralmente i criteri in modo che i criteri coerenti vengano applicati a diverse classi di utenti (ad esempio, quelli locali e su cloud privati e pubblici).*

9. WEB APPLICATION FIREWALL (WAF)*: questa classe di firewall è stata utilizzata sin dalla nascita di applicazioni Web a cui si accede tramite protocolli Web, come HTTP.*

   Un avanzamento delle funzionalità in questa classe di firewall è il filtro URL avanzato.

   Questa è la capacità di rilevare il traffico da URL dannosi e quindi prevenire minacce e attacchi basati sul Web ricevendo dati in tempo reale analizzati da algoritmi di apprendimento automatico.

   In particolare, questa classe di firewall può ispezionare i vettori di minacce per **SQL Injection**, *iniezioni di comandi del sistema operativo e attacchi di cross-site scripting, nonché prevenire gli attacchi in entrata.*

   Sono utilizzati nelle reti di distribuzione dei contenuti CDN *(*CONTENT DELIVERY NETWORKS*) e per prevenire attacchi* DDOS (DISTRIBUTED DENIAL-OF SERVICE).

Alcune funzionalità aggiuntive presenti in questa classe di firewall sono:

1. *Possibilità di specificare un elenco di servizi consentiti (controllo a livello di applicazione);*
2. *Il traffico corrisponde all'intento delle porte consentite;*
3. *Filtraggio di alcuni protocolli indesiderati.*

3.3 – INSIEME DI DISPOSITIVI CON FUNZIONI INTEGRATE

1. GESTIONE UNIFICATA DELLE MINACCE (UNIFIED THREAT MANAGEMENT - UTM)

   I dispositivi UTM combinano molte delle funzioni di sicurezza più critiche – firewall, sistema di prevenzione delle intrusioni (INTRUSION PREVENTION SYSTEM - IPS), *concentratore* VPN, *antivirus gateway, filtraggio dei contenuti e bilanciamento del carico WAN – in un unico dispositivo, di solito con una console di gestione unificata.*

2. FIREWALL DI NUOVA GENERAZIONE NGFW (NEXT GENERATION FIREWALL)

   Questi dispositivi di sicurezza **all-in-one** *si basano sul modello UTM, ma sono combinati con scalabilità e prestazioni di classe enterprise e un focus sull'ispezione granulare del traffico delle applicazioni* **Layer 7**.

   Gli NGFW hanno aggiunto funzionalità per facilitare la segmentazione interna, l'integrazione con i prodotti **sandboxing**, *l'ispezione* SSL (SECURE SOCKETS LAYER) *e la* SD-WAN.

   L'elaborazione all'edge trae vantaggio dai firewall locali, che applicano l'elaborazione in loco.

   Sono più efficienti dal punto di vista energetico rispetto alle macchine virtuali e riducono la latenza perché evitano il "**ROUND TRIP**" *(metodologia per la sincronizzazione delle entità sw) verso il cloud.*

   Gli NGFW *sono dotati di protezione dalle minacce ad alte prestazioni (ad esempio, prevenzione delle intrusioni, filtro Web, antimalware, controllo delle applicazioni) per attacchi noti, ispezione SSL/TLS e antivirus.*

3. PROTEZIONE APPLICAZIONI WEB E API (WEB APPLICATION AND API PROTECTION - WAAP)

   Approccio di sicurezza completo e di un miglioramento rispetto ai firewall delle applicazioni Web (WAF).

WAAP è un componente integrale per la sicurezza api, la difesa BOT *e la protezione DDOS.*

4. GATEWAY WEB SICURO SWG (SECURE WEB GATEWAY)

   Sono dispositivi utilizzati per l'accesso e il controllo basati su policy di applicazioni incentrate su cloud per utenti aziendali in luoghi onnipresenti (ad esempio, sede centrale, filiali, casa, sedi remote).

   Un SWG è fondamentalmente un filtro web che protegge il traffico utente in **USCITA** tramite l'ispezione HTTP o HTTPS.

   Protegge inoltre gli endpoint degli utenti dalle minacce basate sul Web che possono verificarsi quando gli utenti fanno clic su collegamenti a siti Web dannosi o a siti Web infetti da malware.

   Centralizzano il controllo, la visibilità e la reportistica in molte sedi e tipi di utenti.

   Non sostituiscono i WAF, che proteggono i siti Web dagli attacchi in **ENTRATA**.

3.4 - REQUISITI PER GLI STRUMENTI DI AUTOMAZIONE DI RETE

Gli strumenti automatizzano **l'intero ciclo di vita dei processi** *coinvolti:*

a) *nella distribuzione,*
b) *nell'osservabilità/monitoraggio,*
c) *nella raccolta/reportistica di informazioni sulle minacce (ad esempio, nella generazione di avvisi di violazioni della sicurezza per consentire al personale di sicurezza di intervenire tempestivamente) e,*
d) *in alcuni casi, nella correzione automatica*

della rete.

I requisiti per questi strumenti sono descritti di seguito.

Ogni **requisito generico** *è contrassegnato con l'abbreviazione* **NAUT-GR-x**, *mentre ogni* **requisito funzionale** *è contrassegnato con* **NAUT-FR-x**, *dove x in entrambi i tipi di tag sta per la sequenza numerica.*

1. NAUT-GR-1: *Scalabilità per soddisfare il volume, la velocità e la varietà dei paradigmi odierni di distribuzione e manutenzione dello sviluppo di applicazioni.*

   Questo requisito è fondamentale negli ambienti in cui **DevSecOps** *è utilizzato per distribuire non solo le applicazioni ma anche le infrastrutture, queste ultime utilizzando strumenti* IAC (INFRASTRUCTURE-AS-CODE).

Questi strumenti sono resi parte integrante dei flussi di lavoro automatizzati intelligenti chiamati pipeline CI/CD, *che richiamano questi strumenti per distribuire server (elaborazione), rete e infrastruttura di archiviazione.*

Pertanto, questa classe di strumenti di automazione di rete può essere perfettamente integrata nelle corrispondenti pipeline CI/CD.

2. NAUT-GR-2*: Dovrebbero avere la capacità di ridurre al minimo l'intervento umano per la correzione della sicurezza, che è lento e soggetto a errori.*

   In altre parole, più funzionalità di correzione automatizzate integrate nello strumento, meglio è.

I requisiti funzionali minimi degli strumenti di automazione della rete dovrebbero essere:

1. NAUT-FR-1 *(intelligence e protezione avanzate sulle minacce): Gli strumenti dovrebbero avere informazioni avanzate sulle minacce, funzionalità di prevenzione delle minacce in tempo reale per vulnerabilità note e zero day e funzionalità di sandboxing per isolare il traffico dannoso.*
2. NAUT-FR-2 *(sfruttando la conoscenza degli eventi precedenti): Gli strumenti dovrebbero avere funzionalità per abbinare gli eventi attuali a quelli passati e per sfruttare le misure di correzione eseguite per tali istanze nella soluzione corrente. Ciò comporta una riduzione del tempo medio di interruzione.*

Gli strumenti di monitoraggio e osservabilità della rete e gli strumenti IAC *sono classi importanti di strumenti di automazione della rete; i requisiti e il set di funzionalità sono illustrati nelle sottosezioni seguenti.*

3.4.2 - STRUMENTI DI PROVISIONING DI RETE AUTOMATIZZATI

*Il processo di distribuzione iniziale del l'infrastruttura di rete e il successivo aggiornamento sono automatizzati definendo un flusso di lavoro che richiama l'*IaC *(ad esempio, il flusso di lavoro* **GitOps***) come parte di una definizione di pipeline CI/CD.*

I vantaggi di questo approccio per la gestione dell'infrastruttura di rete aziendale per la distribuzione cloud multi sono i seguenti:

1. *Consente all'azienda di avere uno stretto controllo della versione (monitoraggio delle modifiche) in modo che i dispositivi di rete non autorizzati e le modifiche non autorizzate nelle configurazioni associate non aprono vulnerabilità di sicurezza.*
2. *Consente all'azienda di disporre di un'infrastruttura uniforme in tutti gli ambienti di sviluppo, test, staging e produzione.*

3. *Monitoraggio della deriva* – Drift Monitoring - *(i cambiamenti non intenzionali) tra l'infrastruttura definita (come trovato in* IaC*) e l'infrastruttura operativa e l'adozione di azioni correttive per affrontare la deriva aiutano a mantenere la posizione di sicurezza necessaria per l'ambiente di rete aziendale.*
4. *Il paradigma DevSecOps costituito da pipeline CI/CD richiama la rete strumento di provisioning (generatore di codice IaC) per automatizzare la distribuzione iniziale e successiva riconfigurazione dell'infrastruttura di rete.*

   Poiché le pipeline hanno un processo audit integrato, le modifiche nella configurazione di rete sono automaticamente acquisite nell'audit, che a sua volta consente all'azienda di dimostrare la conformità ai criteri di sicurezza aziendali e la conformità ai criteri normativi per le proprie reti, ove applicabile.
5. *Test del codice (codice IaC) generato dagli strumenti IaC (e richiamato dalla pipeline CI/CD codice che distribuisce l'infrastruttura utilizzando IaC) garantisce che i criteri di sicurezza siano applicati in modo coerente e uniforme all'intera infrastruttura di rete aziendale (ovvero più servizi cloud).*
6. *Il vantaggio di avere plug-in per definire il provisioning di rete per diversi pubblici ambienti provider cloud è che possono essere utilizzati per personalizzare gli strumenti di osservabilità utilizzato per il monitoraggio della rete per ciascuno dei servizi cloud a cui l'azienda si è abbonata.*

3.5 – DISPOSITIVI DI RETE COME SERVIZI

Un'altra tendenza nel panorama della rete aziendale è che una parte dell'infrastruttura di essa può essere ottenuta come servizio in leasing chiamato NETWORK AS A SERVICE (NAAS) *da provider di terze parti.*

Questo servizio è offerto utilizzando tecnologie come il 5G aziendale e l'Edge computing.

I vantaggi di NAAS *sono i seguenti:*

1. *Proprio come gli abbonamenti a SaaS e IaaS, riduce i costi di* **capex** *per l'azienda.*
2. *Essendo software-defined e virtualizzato, è flessibile e scalabile.*
3. *Come conseguenza del vantaggio precedente, i requisiti QoS di diverse applicazioni possono essere soddisfatti creando un flusso di traffico personalizzato per ogni tipo di applicazione.*

4. *Le nuove applicazioni che richiedono un maggiore ingombro di rete possono essere introdotte rapidamente in l'impresa (agilità), facilitando così la diversificazione del business.*

4 - CONFIGURAZIONI DI RETE PER AMBIENTI APPLICATIVI IBRIDI

*Le funzionalità di configurazione di rete (*NETWORK CONFIGURATION FEATURES - NCF*) riscontrato nelle aziende con ambienti applicativi ibridi possono essere classificate nelle seguenti aree:*

1. Configurazione di rete per la gestione dei dispositivi *(*DEVICE MANAGEMENT*).*
2. Configurazione di rete per l'autenticazione utente *(*USER AUTHENTICATION*).*
3. Configurazione di rete per l'autenticazione dei dispositivi e il monitoraggio dello stato *(*DEVICE AUTHENTICATION AND HEALTH MONITORING*).*
4. Configurazione di rete per l'autorizzazione dell'accesso alle applicazioni (AUTHORIZING APPLICATION ACCESS)
5. Configurazione di rete per la prevenzione dell'escalation degli attacchi *(*PREVENTING ATTACK ESCALATION - MICROSEGMENTATION*).*

Ciascuna delle funzionalità di configurazione di rete è enumerata utilizzando l'identificatore del formato **HAENCF-x**, *dove* **HAE** *(*HYBRID APPLICATION ENVIRONMENT*) indica un ambiente applicativo ibrido,* **NCF** *(*NETWORK CONFIGURATION FEATURE*) indica la funzionalità di configurazione di rete e* **x** *sta per il numero di sequenza della funzionalità.*

4.1 - CONFIGURAZIONE DI RETE PER LA GESTIONE DEI DISPOSITIVI

Con la **scomparsa del perimetro di rete e la distribuzione dei target applicativi** *(essendo un ambiente applicativo ibrido), le aziende dovrebbero adottare un paradigma* "ENDPOINT È IL PERIMETRO" *e disporre di un sistema di gestione dei dispositivi.*

HAE-NCF-1*: tutti gli endpoint che accederanno alle applicazioni locali e basate su cloud devono essere gestiti utilizzando una rete di gestione dedicata.*

Le attività gestite minime dovrebbero includere:

a) Installazione e manutenzione dei certificati di autenticazione del dispositivo e del servizio;

b) Installazione e manutenzione di applicazioni per la salute dei dispositivi;

c) Aggiornamenti delle patch sui dispositivi;

d) *Creazione e manutenzione di pagine bianche che contengano mappature dispositivo/servizio per prevenire il dirottamento del servizio* (SERVICE HIJACKING)*, impedendo l'ingresso a server dannosi o compromessi che si presentano come host legittimi per i servizi.*

4.2 - CONFIGURAZIONE DI RETE PER L'AUTENTICAZIONE UTENTE

HAE-NCF-2*: La rete deve essere configurata per instradare la richiesta di accesso dell'utente a destinazioni diverse per l'autenticazione dell'utente, a seconda dell'applicazione di destinazione a cui si accede.*

a) *Quando la richiesta di accesso dell'utente riguarda un'applicazione basata su cloud (ad esempio,* SaaS*), l'utente deve essere* **indirizzato all'IdP aziendale**.
Quando la richiesta di accesso dell'utente riguarda un'applicazione Web locale, l'utente deve essere **indirizzato a un gateway Web (proxy inverso)**.
Questo reindirizzamento può essere influenzato attraverso un processo chiamato split DNS.
Se un certificato digitale è utilizzato come primo fattore di autenticazione, l'IdP deve verificare la validità dell'utente certificato (stato corretto e non scaduto) tramite meccanismi quali chiamate CRL, OCSP o Active Directory.

b) *Per autenticare gli utenti è necessario utilizzare almeno due fattori di autenticazione.*
Se il possesso di un certificato valido è il primo fattore, allora il riconoscimento di un messaggio **push** *(utilizzando tecnologie come DuoMobile, TouchID o Yubikey) o* **OTP** *al telefono cellulare può essere utilizzato come secondo fattore.*

4.3 - CONFIGURAZIONE DI RETE PER L'AUTENTICAZIONE DEI DISPOSITIVI E IL MONITORAGGIO STATO

1. HAE-NCF-3*: L'autenticazione del dispositivo può essere eseguita tramite la convalida del certificato utilizzando protocolli appropriati.*
È possibile eseguire un controllo dello stato del dispositivo richiamando l'applicazione residente.

2. HAE-NCF-4: *Le applicazioni basate su microservizi (locali o nel cloud) devono avere proxy di servizio installati con ogni servizio per fornire la connettività necessaria per la comunicazione tra servizi oltre a eseguire servizi di autenticazione e autorizzazione per ogni richiesta di servizio.*

4.4 - CONFIGURAZIONE DI RETE PER L'AUTORIZZAZIONE DELL'ACCESSO ALLE APPLICAZIONI

HAE-NCF-4: *I protocolli standardizzati, come* **OAuth 2.0**, *devono essere utilizzati per emettere token di accesso all'utente, al dispositivo o al servizio convalidato per consentire l'accesso alle applicazioni basate su cloud.*

4.5 - CONFIGURAZIONE DI RETE PER PREVENIRE L'ESCALATION DEGLI ATTACCHI (MICROSEGMENTAZIONE)

La microsegmentazione è una pratica di progettazione della sicurezza in cui una rete interna (ad esempio, nel data center, nella regione del provider cloud) è divisa in segmenti isolati in modo che il traffico in entrata e in uscita da ciascun segmento possa essere monitorato e controllato.

Le entità abilitate dalla microsegmentazione sono:

1. **Attento Monitoraggio del traffico consentito dai segmenti isolati e relativamente piccoli che ne permettono una migliore visibilità**.

Ne consegue che

2. *Il controllo granulare degli accessi è possibile definendo i criteri associati.*

L'abilitazione delle funzionalità di cui sopra GARANTISCE IL LIMITE AL MOVIMENTO LATERALE (EST-OVEST) NON AUTORIZZATO *di un utente o di un'applicazione che ha:*

a) **violato il perimetro** *per entrare nella rete interna*

oppure

b) **è stato avviato da utenti all'interno della rete interna stessa**.

4.5.1 - PREREQUISITI PER L'ATTUAZIONE DELLA MICROSEGMENTAZIONE

1. CREAZIONE DELL'IDENTITÀ DELL'APPLICAZIONE

Requisito fondamentale per abilitare questo è l'assegnazione di un'identità univoca a ciascuna applicazione o servizio, proprio come ogni utente porta un'identità univoca (ad esempio, userid).

Prima dell'era delle applicazioni basate su cloud, le richieste di applicazione venivano convalidate in base alla subnet IP o all'indirizzo IP da cui provenivano.

L'accesso onnipresente e i multi-cloud hanno eliminato il concetto di perimetri di rete. Pertanto, l'autenticazione e l'autorizzazione basate su tali parametri non sono né fattibili né scalabili.

Inoltre, la presenza di proxy, la conversione degli indirizzi di rete e i servizi di bilanciamento del carico **rendono impossibile per l'applicazione chiamata conoscere l'indirizzo IP dell'applicazione chiamante al fine di prendere decisioni di autenticazione o autorizzazione.**

Un'identità applicativa univoca è inevitabile.

2. DEFINIZIONE DELL'ATTENDIBILITÀ NELL'IDENTITÀ DELL'APPLICAZIONE

L'*identità dell'applicazione creata non deve essere soggetta a spoofing e deve essere continuamente verificabile.*

Pertanto, è necessaria un'identità crittografica sotto forma di chiave pubblica contenuta in un certificato emesso da una fonte attendibile per soddisfare questi criteri.

*La verifica dell'autenticatore associato a questa identità viene eseguita dalla parte autenticante inviando una sfida e l'assicurazione contro l'attacco di riproduzione per il processo di autenticazione è garantita inviando un "***nonce***" allegato alla sfida.*

È necessario mantenere una directory protetta che fornisce un mapping del servizio al server di hosting per garantire che le applicazioni o i servizi siano ospitati solo su server autorizzati e che non esistano versioni spurie dei servizi.

3. INDIVIDUAZIONE DELLE RISORSE DELL'APPLICAZIONE

Dovrebbe esserci un mezzo solido per scoprire tutte le risorse dell'applicazione (ad esempio, servizi, reti, ecc.).

4. SEGMENTAZIONE DEI CARICHI DI LAVORO

I requisiti di sicurezza per tutte applicazioni e servizi devono essere identificati e raggruppati; i raggruppamenti devono essere stabiliti in base a requisiti di sicurezza identici.

5. MAPPING DEI RAGGRUPPAMENTI LOGICI DI APPLICAZIONI A INFRASTRUTTURE FISICHE O VIRTUALI

   I raggruppamenti incentrati sulle applicazioni devono essere mappati a infrastrutture fisiche o virtuali che costituiscono la topologia del data center al fine di facilitare la distribuzione effettiva di applicazioni e servizi.

4.5.2 - MICROSEGMENTAZIONE – APPROCCI DI ATTUAZIONE

Per implementare la microsegmentazione si utilizzano i seguenti approcci.

1. APPROCCIO BASATO SU SEGMENTI

   In questo approccio, le applicazioni e le risorse di servizi con requisiti di sicurezza simili sono raggruppate in un segmento univoco e sono create regole firewall per bloccare o consentire la comunicazione con ciascun gruppo o segmento.

   I segmenti sono creati utilizzando astrazioni a livello di rete, come ID VLAN o altri approcci di tagging, mentre i criteri vengono definiti utilizzando costrutti di indirizzi di rete (ad esempio, indirizzi IP e porte).

   I criteri si applicano alle **subnet** *(ad esempio, le VLAN) e non ai singoli host.*

   Ogni segmento è protetto da dispositivi gateway, come switch e router intelligenti o firewall di nuova generazione (NGFW), che dovrebbero avere la capacità di reagire e adattarsi in risposta alle minacce e ai cambiamenti nei flussi di lavoro delle applicazioni.

   I gateway di segmentazione monitorano il traffico, bloccano le minacce e applicano l'accesso granulare al traffico est-ovest (raramente per il traffico nord-sud) all'interno di data center locali o regioni cloud.

   La difficoltà principale con questo approccio è la difficoltà nel mappare i segmenti basati sui requisiti di sicurezza delle applicazioni creati ai segmenti di rete corrispondenti.

   Un diagramma schematico della microsegmentazione segmentale è mostrato nella Figura 1.

   Ogni microsegmento numerato nella figura è una VLAN univoca identificata da un ID VLAN.

   Il gruppo di applicazioni che saranno eseguite in quel particolare segmento VLAN può essere definito utilizzando criteri diversi.

   Uno dei criteri è "**tutte le applicazioni con requisiti di sicurezza simili**".

Un altro è che "**tutti i livelli (frontend Web, server logici dell'applicazione e server di database) associati a una particolare applicazione**" *dovrebbero essere eseguiti in un singolo microsegmento, come mostrato nella figura.*

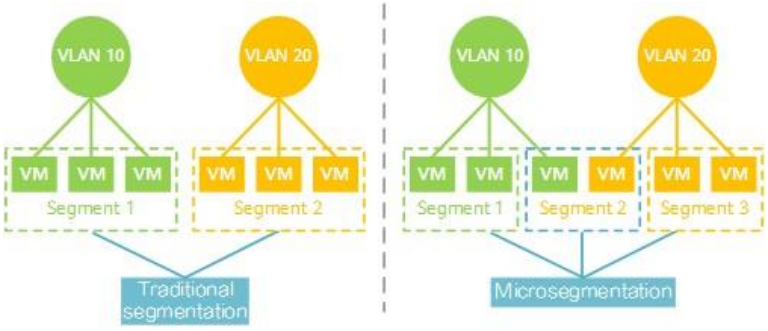

FIG. 1. MICROSEGMENTAZIONE SEGMENTALE

2. APPROCCIO BASATO SU SERVER VIRTUALIZZATO

Questo approccio è applicabile solo alle reti che contengono server virtualizzati poiché è implementato nell'hypervisor.

Esistono due possibili meccanismi:

1 *Utilizzo di firewall virtuali all'interno di un hypervisor per isolare il traffico destinato a diverse VM all'interno dell'hypervisor.*

2 *Utilizzo di tecniche di incapsulamento per creare sovrapposizioni (ad esempio, VXLAN) che sono eseguite su una rete di* **underlay** *(sub strato) costituita da designazioni di indirizzi IP; i criteri di controllo di accesso sono applicati all'hypervisor stesso all'esterno del carico di lavoro (applicazione o microservizio).*

3. MICROSEGMENTAZIONE BASATA SU HOST

In alternativa (o in aggiunta), la microsegmentazione basata su host può essere implementata utilizzando agenti software sugli artefatti dell'endpoint (ad esempio, i server).

Sfrutta la funzionalità firewall nativa integrata nell'host.

Gli agenti software possono sovrapporre una rete segmentata software-definita tra data center, cloud, bare metal e ambienti ibridi.

L'agente fornisce consapevolezza del contesto e visibilità per ogni carico di lavoro e, di conseguenza, consente la definizione e l'applicazione di criteri granulari.

4. MICROSEGMENTAZIONE BASATA SULL'IDENTITÀ

I criteri di microsegmentazione basati sull'identità utilizzano identificatori contestuali basati sull'applicazione (ad esempio, il servizio front-end di elaborazione degli ordini può comunicare con il servizio back-end dell'inventario) anziché parametri di rete (consentire chiamate dalla subnet 192.168.10.x alla versione 10.0.0.31).

Gli identificatori assegnati ai servizi sono identità crittografiche, che vengono utilizzate per l'autenticazione e l'autorizzazione reciproche durante ogni richiesta e risposta al servizio.

I vantaggi di questo tipo di microsegmentazione sono:

1. *I criteri basati sulle identità di servizio/applicazione non utilizzano variabili correlate all'infrastruttura (ad esempio, indirizzi IP, subnet e così via), quindi* questi criteri sono indipendenti dall'ambiente e offrono la libertà per i servizi/applicazioni *da migrare in ambienti diversi e mantengono comunque gli stessi criteri.*
2. *L'indipendenza delle policy dall'infrastruttura consente di testarle semplicemente esercitando l'applicazione e osservando i risultati (ad esempio, traccia della sequenza di chiamate di servizio e richieste/risposte invece di configurare correttamente l'infrastruttura per le esecuzioni dei test).*
3. *Le policy di microsegmentazione possono essere definite/implementate incorporando il codice in flussi di lavoro automatizzati, come le pipeline CI/CD per mezzo della disponibilità di strumenti per la specifica dichiarativa delle policy attraverso strumenti* "POLICY AS CODE".
4. *La microsegmentazione consente un controllo granulare (grana fine) degli accessi fornendo visibilità alle sequenze/interdipendenze delle chiamate delle applicazioni e ai flussi di dati attraverso il tracciamento a livello di host, consentendo così l'applicazione di policy di sicurezza per il traffico delle applicazioni che è sia* **NORD-SUD** *che* **EST-OVEST**, *indipendentemente dall'ambiente (ad esempio, data center aziendale o infrastruttura cloud).*

Il motivo per cui la microsegmentazione basata sull'identità è studiata nel panorama delle reti aziendali è che consente solo un traffico di rete valido tra i vari servizi componenti dell'applicazione a causa dell'autenticazione e dell'autorizzazione reciproche utilizzando le identità del servizio, consentendo così di raggiungere gli obiettivi dell'accesso alla rete Zero Trust (ZTNA).

4.6 - FRAMEWORK DI SICUREZZA CHE REGOLANO LE CONFIGURAZIONI DI RETE

*Esempi di tali framework sono il perimetro definito dal software (*SOFTWARE DEFINED PERIMETER - SDP*) e l'accesso alla rete* ZERO TRUST *(ZTNA).*

4.6.1 - BASI CONCETTUALI – INFORMAZIONI CONTESTUALI

*È stato ampiamente riconosciuto che la convalida dell'identità è il punto di ingresso (***può essere un altamente vulnerabile***) a una richiesta di applicazione poiché tutte le richieste, provenienti da un servizio (o microservizio), da un utente o da un dispositivo, sono fornite con un'identità rivendicata.*

Questa identità deve essere verificata utilizzando un'**autenticazione a più fattori robusta e resistente al phishing**.

Tuttavia, sono necessari e **sono collettivamente denominati informazioni contestuali altri attributi associati all'utente ed anche le informazioni associate ad altre entità coinvolte in una richiesta di accesso all'applicazione**, *ad esempio dispositivi e servizi.*

Poiché il ruolo delle INFORMAZIONI CONTESTUALI *nei potenziali attacchi potrebbe non essere noto, l'insieme da includere nella decisione di accesso è una decisione basata sul rischio.*

Le INFORMAZIONI CONTESTUALI *possono in linea di massima appartenere alle seguenti cinque aree chiave:*

1. INFORMAZIONI SULL'UTENTE CHE RICHIEDE L'ACCESSO

   a) *Identità dell'utente.*
   b) *Attributi associati all'utente: ruolo nell'organizzazione, le assegnazioni correnti e lo stato (verifica incrociata dell'identità nella directory IDM aziendale rispetto alla directory aziendale).*

2. INFORMAZIONI SUL DISPOSITIVO DA CUI VIENE RICHIESTO L'ACCESSO

   Stabilire la fiducia nel dispositivo attraverso una combinazione di profili di salute e di rischio del dispositivo.

   *Ad esempio, il profilo di rischio del dispositivo può essere ottenuto attraverso un controllo della "***postura fuori dagli schemi***" predefinito (rischio del dispositivo) con o senza integrazione con uno strumento di protezione degli endpoint per il dispositivo.*

   *Altre informazioni cruciali (***fornite dai dati di telemetria***) necessarie per valutare lo stato di sicurezza dei dispositivi endpoint includono:*

   a) *l'etichetta di supporto del dispositivo (il dispositivo è gestito o di proprietà dell'azienda) e*

b) le informazioni sulla postura del dispositivo (se è stato compromesso).

Tutti questi fattori entrano in una valutazione delle politiche per determinare il livello di attendibilità e devono essere incanalati nelle decisioni di autenticazione e monitoraggio.

3. INFORMAZIONI SUI DATI CONTESTUALI IN TEMPO REALE

   Data, ora e geolocalizzazione in cui si verifica la richiesta di accesso.

4. INFORMAZIONI SUI SERVIZI IT

   Ad esempio, app, dati, ecc. a cui si accede.

5. INFORMAZIONI SULLA SICUREZZA DELL'AMBIENTE CHE OSPITA I SERVIZI IT A CUI SI ACCEDE.

Requisiti per le informazioni contestuali:

1. *Dovrebbe includere non solo ciò che viene raccolto dalla piattaforma nativa (la piattaforma su cui è ospitata l'applicazione) ma anche quello che può essere ottenuto da piattaforme di terze parti e può fornire informazioni più dettagliate.*
2. *Dovrebbe essere disponibile in tempo reale in modo che l'esperienza utente con l'accesso non sia influenzata.*
3. *Dovrebbe essere prioritario in base al valore che ciascuno fornisce.*
4. *Dovrebbe essere coerente con il livello di rischio associato a ciascuna richiesta di accesso.*

4.6.2 - FRAMEWORK SICUREZZA RETE –SOFTWARE DEFINED PERIMETER (SDP)

Una base concettuale per l'accesso sicuro alla rete alle risorse IT è il perimetro definito dal software (SDP).

In SDP, la separazione tra le reti non è definita dal gruppo di indirizzi di rete o dalle VLAN, il che la rende indipendente dalla rete.

È definita logicamente e dinamicamente per ogni utente e ogni particolare richiesta.

In altre parole, **per ogni richiesta dell'utente, il sottoinsieme di risorse IT a cui l'utente ha accesso è allocato dinamicamente indipendentemente dalla posizione della risorsa** (ad esempio, data center aziendale, filiale, cloud privato o pubblico, ecc.).

I principi salienti di SDP includono:

1. Il concetto SDP consiste nel rendere invisibili tutte le risorse IT *(ad esempio, porte, carichi di lavoro e applicazioni)* e renderle note e accessibili solo dopo che l'utente è stato autenticato e autorizzato.

   Viene stabilita solo una connessione di rete tra l'utente e le risorse IT consentite, seguendo così il principio del privilegio minimo.

   Il livello di accesso determinato dal processo precedente è continuamente rivalutato durante la sessione utente e ricalibrato se necessario.

   In altre parole, man mano che il contesto che circonda l'identità cambia in tempo reale, così possono cambiare i diritti dell'utente.

2. Ridurre la superficie d'attacco impedendo il movimento laterale (EST-OVEST) attraverso tecniche come la microsegmentazione, *come descritto nella Sezione 4.4.*

   Con la crescente distribuzione di microservizi, le richieste di risorse tra servizi (generatore di traffico **EST-OVEST***) dominano le richieste di applicazioni esterne (traffico* **NORD-SUD***).*

   L'applicazione di questo principio garantisce quindi il traffico **EST-OVEST** *(interno).*

4.6.3 - FRAMEWORK SICUREZZA RETE – **ZERO TRUST NETWORK ACCESS (ZTNA)**

ZTNA *è la conseguenza di un'architettura* ZERO TRUST, *che a sua volta è una realizzazione dei* PRINCIPI di ZERO TRUST.

Il NIST definisce ZERO TRUST *e i* PRINCIPI *di* ZERO TRUST *come:*

1. ZERO TRUST (ZT) *è il termine per un insieme in evoluzione di paradigmi di sicurezza informatica che spostano le difese da perimetri statici basati sulla rete per concentrarsi su utenti, beni e risorse.*

   È un insieme di primitive di sicurezza piuttosto che un particolare insieme di tecnologie.

   ZERO TRUST *presuppone che non vi sia alcun trust (garanzia scontata!) implicito concesso alle risorse o agli account utente in base esclusivamente al loro percorso fisico o di rete (ad esempio, reti locali rispetto a Internet) o in base alla proprietà delle risorse (aziendale o di proprietà personale).*

   ZERO TRUST *si concentra sulla protezione delle risorse (ad esempio, risorse, servizi, flussi di lavoro, account di rete, ecc.) piuttosto che sui segmenti di rete,* **poiché il percorso di rete non è più visto come il componente principale della posizione di sicurezza della risorsa**.

2. *Un'architettura* ZERO TRUST *(ZTA) utilizza i principi ZT per pianificare l'infrastruttura e i flussi di lavoro industriali e aziendali.*

Le linee guida del NIST su ZTA [NIST SP 800-207] contengono una definizione astratta di architettura zero trust (ZTA) e forniscono modelli di distribuzione generali e casi d'uso in cui lo ZERO TRUST *potrebbe migliorare la posizione generale di sicurezza della tecnologia dell'informazione di un'azienda.*

Dalla visione NIST di ZTA e dalle implementazioni dello stato di pratica, sono emersi i seguenti elementi costitutivi di ZTA:

1. CLIENT O BROWSER*: il punto di ingresso per tutti gli utenti per accedere a qualsiasi risorsa ospitata in ambienti multi-cloud e on-premise.*
2. CONTROLLER*: il motore decisionale dei criteri, che gestisce i criteri, le condizioni e i diritti che concedono l'accesso a tutti gli utenti, i dispositivi e i carichi di lavoro da un singolo dashboard o tramite API.*
3. GATEWAY*: il punto di applicazione dei criteri.*

   I gateway controllano il flusso di accesso alle risorse protette e costruisce dinamicamente regole di microsegmentazione basate sui diritti concessi.

In tutti i framework di sicurezza per gli attuali ambienti di rete aziendali, i principi comuni che sono alla base dei requisiti specifici dell'applicazione, come:

a) BASSA LATENZA,
b) ELEVATE VELOCITÀ DI TRASFERIMENTO DEI DATI E
c) ALTA AFFIDABILITÀ,

sono applicabili nei precedenti scenari di rete e rimangono gli stessi.

5 - INFRASTRUTTURA WAN SICURA

I consorzi industriali utilizzano il termine SECURE ACCESS SERVICE EDGE (SASE) *per riferirsi a un quadro completo che offre reti wide area e vari servizi di sicurezza.*

*SASE può essere considerato come la controparte di rete della "*MESH*" di servizi dell'applicazione, che fornisce un set completo di servizi applicativi, inclusa la sicurezza per le applicazioni native del cloud.*

Sulla base della discussione di cui sopra, questa sezione si concentrerà sui seguenti argomenti:

1. *Requisiti per una SD-WAN sicura;*
2. *Requisiti per un'architettura di servizi di sicurezza integrata per SD-WAN.*

5.1 - REQUISITI COMUNI PER UNA SD-WAN SICURA

*Oltre alle VPN fornite da CSP, una tecnologia di rete che fornisce connettività di rete per l'accesso a servizi basati su cloud per le aziende è la rete SD-WAN (*SOFTWARE-DEFINED WIDE AREA NETWORKING*).*

Gli obiettivi di progettazione e le caratteristiche comuni in tutte le offerte SD-WAN includono:

1. AMPIA CONNETTIVITÀ

   Per connettere in modo sicuro gli utenti che si trovano ovunque (ad esempio, casa, sede pubblica, filiale, ufficio aziendale, ecc.) ad applicazioni e risorse ospitate ovunque (ad esempio, data center, servizi cloud singoli o multipli) utilizzando qualsiasi trasporto WAN (ad esempio, MPLS, Internet a banda larga, 4G, LTE, 5G wireless).

2. CONSAPEVOLEZZA DELLE APPLICAZIONI

   Per monitorare il traffico di rete e scegliere dinamicamente il percorso migliore disponibile in base:

   a. *al tipo di traffico di rete,*
   b. *alle condizioni di carico della rete e*
   c. *alla priorità aziendale dell'applicazione.*

   Questa funzionalità è abilitata utilizzando tecniche quali:

   a. *utilizzo della larghezza di banda,*
   b. *bilanciamento del carico e l'ottimizzazione della velocità riducendo jitter,*
   c. *latenza e perdita di pacchetti.*

   Affrontare la priorità aziendale dell'applicazione è possibile solo se la soluzione SD-WAN è in grado di identificare diversi tipi di applicazioni (ad esempio, applicazioni di messaggistica / e-mail, applicazioni di social media, applicazioni generali relative allo storage, applicazioni della supply chain) e allocare di conseguenza le priorità di routing e le risorse WAN.

3. INTEGRAZIONE DI FUNZIONI DI SICUREZZA E DI RETE

   Utilizzo di dispositivi che contengano una combinazione di funzioni di rete e di sicurezza (ad esempio, la presenza di un firewall e di funzioni di gateway Web sicuro [SWG] in un router WAN).

4. VISIBILITÀ CENTRALIZZATA E FUNZIONALITÀ DI GESTIONE

   Include la possibilità di riconoscere e autenticare i dispositivi appena connessi e portarli sotto i flussi di lavoro di gestione definiti come nodi in modo da configurare un set uniforme di policy che copra tutti i componenti.

5. INTEGRAZIONE CON POSTAZIONI LAN REMOTE

   Un'ulteriore caratteristica preferita ma non essenziale è l'integrazione delle funzioni WAN e LAN in un unico dispositivo (quest'ultimo denominato SD-Branch), che può essere gestito utilizzando un'unica console di gestione, fornendo così una migliore visibilità su entrambi i componenti.

   Questa funzionalità consente la connettività di SD-WAN nella LAN locale presso le filiali remote.

5.2 - REQUISITI SPECIFICI WAN PER ACCESSO AL CLOUD

Le aziende possono ottenere l'accesso al cloud in due modi:

1. *attraverso i servizi VPN forniti dai provider cloud o*
2. *integrando la propria SD-WAN con le reti private dei provider cloud, spesso chiamate WAN cloud.*

Il vantaggio del secondo approccio è che le aziende possono estendere le loro WAN esistenti all'interno e attraverso la rete privata di un provider cloud, consentendo una rete aziendale coerente e l'applicazione delle policy di sicurezza.

Due dei vantaggi di questa estensione sono:

1. *Visibilità completa end-to-end tra "endpoint di accesso" e endpoint di risorse IT (applicazione o dati) anche se quest'ultimo si trova nella rete di un provider cloud.*
2. *Applicazione della logica di segmentazione della rete distribuita per l'accesso alle risorse locali alle risorse basate su cloud.*

Questa orchestrazione della rete privata del provider cloud può essere ottenuta progettando una RETE DI OVERLAY *personalizzata sulla rete del provider cloud come rete sottostante.*

Questa funzionalità è subordinata al fatto che i CSP offrano integrazioni API per diverse offerte SD-WAN.

È emersa un'architettura per la gestione di reti aziendali connesse a più CSP.

Una parte del settore definisce la raccolta di dispositivi in questa architettura una piattaforma di rete cloud.

I requisiti per questa piattaforma di rete multi-cloud sono:

1. *Fornire visibilità operativa e controllo comuni sull'accesso alla rete nativa fornito da più provider cloud.*

   Al fine di fornire un'architettura di rete in grado di "attraversare i cloud", è necessario:

   a. sfruttare *le funzionalità native del cloud (in particolare i costrutti di rete cloud nativi) di ciascun cloud;*
   b. astrarre *tale funzionalità con le API;*
   c. aggiungere *funzionalità avanzate del piano dati per alta disponibilità, sicurezza e visibilità/controllo operativo;*
   d. fornire *gli strumenti per gestire queste funzionalità in modo dinamico o automatico.*

2. *Fornire una politica di sicurezza comune in entrata e in uscita per gli ambienti applicativi (ad esempio, VPC, VNET, VVN, ecc.) su cloud.*
3. *Abilitare la crittografia end-to-end all'interno del cloud e la crittografia ad alte prestazioni dal data center al cloud.*
4. *Supportare l'automazione per la distribuzione e la configurazione.*

Sulla base dei requisiti di cui sopra, sono emerse offerte di piattaforme di rete multi-cloud con i seguenti elementi architetturali:

1. *Un livello di astrazione che si trova sopra l'accesso alla rete nativa offerto dai singoli CSP ai loro servizi.*

   Questo livello consente all'azienda di gestire l'intera rete aziendale, costituita da connettività a più cloud, connessioni intra-cloud e strutture di rete di data center locali, come un'unica unità. Per consentire ciò, è necessaria una visibilità completa dell'intero panorama della rete aziendale. Quindi, questo livello ha bisogno di input da sofisticati strumenti di osservabilità e monitoraggio per svolgere le sue funzioni.
2. *La scelta di una configurazione dell'infrastruttura (ad esempio, la configurazione del cloud privato virtuale con segmenti di rete isolati) per l'hosting di applicazioni nell'infrastruttura di rete fornita dal CSP è facilitata da una classe di strumenti chiamati strumenti IaC, che hanno funzionalità con definizioni di configurazione di rete dei principali CSP integrati come plug-in. Ciò facilita il provisioning iniziale delle risorse di rete e la successiva modifica della configurazione di rete e delle risorse per l'hosting di applicazioni aziendali nei cloud.*

Esistono quattro tendenze del settore che possono avere implicazioni per la sicurezza in relazione alla SD-WAN:

1. *L'accesso SD-WAN è acquisito come servizio basato su cloud tipo* NETWORK AS A SERVICE (NAAS), *proprio come* IAAS *e* SAAS.

2. *Gli algoritmi basati sull'*IA *sono utilizzati per monitorare le reti per le condizioni relative alla sicurezza; per misure di miglioramento della resilienza, come la limitazione per determinate destinazioni; e per le decisioni di routing dinamico per mantenere i parametri QoS, come latenza e larghezza di banda.*
3. *Le reti wireless sono utilizzate per la connettività dell'ultimo miglio utilizzando una rete di accesso radio 5G (RAN).*
4. *Le funzionalità di accesso remoto sicuro fornite da tecnologie come VPN sono combinate in SD-WAN.*

5.3 – REQUISITI ARCHITETTURA SERVIZI SICUREZZA INTEGRATA PER SD-WAN

Un'architettura di servizi di sicurezza integrata per SD-WAN ha conglobato al suo interno funzioni sia di rete sia di sicurezza.

Le funzionalità di accesso alla rete e le funzioni di sicurezza sono offerte come servizio cloud accessibile alle aziende attraverso posizioni di rete strategiche distribuite su una vasta area chiamata POINT OF PRESENCE (POP).

Il termine coniato da Gartner nel 2019 indica un'architettura che converge le funzioni di rete e di sicurezza ed è fornita su scala globale come servizio cloud, si definisce: SECURE ACCESS SERVICE EDGE (SASE).

I servizi di rete e di sicurezza forniti da un servizio chiamato SASE non sono nuovi, ma semplicemente forniti insieme come un unico pacchetto anziché attraverso soluzioni di sicurezza puntuale (capitolo 3).

I vari punti di connettività dall'azienda ai PoP SASE sono chiamati ENTERPRISE EDGE.

Nei margini aziendali possiamo trovare:

1. CLIENT *(utenti che accedono tramite desktop, laptop e dispositivi mobili da filiali o postazioni remote come Home o IoT).*
2. RISORSE IT *(app interne ospitate in data center o filiali, app basate su cloud (SaaS, IaaS)).*

L'infrastruttura di rete SASE diventa quindi parte integrante della rete aziendale ogni volta che uno o più edge aziendali si connettono a vari PoP del servizio cloud SASE.

Le tre funzioni principali fornite da SASE sono:

1. OTTIMIZZAZIONE DEL TRAFFICO DI RETE PER DIVERSI TIPI DI TRAFFICO*: Riduzione della latenza e miglioramento della disponibilità.*
2. CONTROLLO DEGLI ACCESSI PER L'ACCESSO A DIVERSI TIPI DI RISORSE IT*: Applicazioni, Database ecc.*

3. PREVENZIONE DELLE MINACCE: *Monitoraggio, raccolta di informazioni su minacce e attacchi, azioni correttive.*

Alcune delle caratteristiche strutturali delle offerte SASE sono:

1. PUNTO DI PRESENZA DISTRIBUITO A LIVELLO GLOBALE (POINT OF PRESENCE - POP): *un servizio SD-WAN globale con una propria rete* BACKBONE *privata costituita da PoP in tutto il mondo destinati a ridurre al minimo i problemi di latenza.*
2. AGENTE DI SICUREZZA SUI DISPOSITIVI: *l'agente di sicurezza sul dispositivo dell'utente finale prende decisioni di rete e dirige il traffico da diverse applicazioni.*

   Le funzionalità specifiche includono consentire o negare dinamicamente le connessioni a servizi e applicazioni in base alle regole di business definite da un'organizzazione.

Di seguito sono riportati i servizi di sicurezza minimi disponibili in un'architettura integrata:

1. *Servizi firewall*
2. *Servizi gateway Web sicuri*
3. *Servizi anti-malware*
4. *Servizi IPS*
5. *Servizi CASB*
6. *Servizi DLP*

Alcune delle funzionalità di sicurezza avanzate presenti nelle offerte SASE includono:

1. TECNOLOGIA DI ISOLAMENTO DEL BROWSER: *è spesso combinata con soluzioni di gateway Web sicure e fornisce una migliore sicurezza delle attività Web per affrontare le minacce in tempo reale.*
2. STRATEGIA DI VALUTAZIONE ADATTIVA CONTINUA DEL RISCHIO E DELLA FIDUCIA (CARTA): *questa strategia prevede sessioni di monitoraggio costante ed esegue analisi adattive del comportamento sul monitoraggio per modificare dinamicamente i livelli di sicurezza e le autorizzazioni se il profilo di attendibilità (ad esempio, deficit di attendibilità) di un dispositivo cambia.*

RIFERIMENTI

1) NIST SP 800-207 – Zero Trust Architecture
2) NIST SP 800-215 – Guide to Secure Enterprise Network Landscape