Allegato E

Procedura operativa per la richiesta e modifica VPN presso ASST 'Papa Giovanni XXIII'

Data emissione: 12/01/2022
Revisione: 15

Indice generale

1 Introduzione

NOTE IMPORTANTI:

- Si informa che i Personal Computer che vengono utilizzati per connettersi in VPN all'infrastruttura IT dell'Ente “ASST Papa Giovanni XXIII” devono obbligatoriamente avere installato un sistema di End Point Security/Antivirus aggiornato e devono obbligatoriamente essere aggiornati per quanto riguarda le patch del sistema operativo e altro SoftWare eventualmente installato. Entrambe le misure di sicurezza (Antivirus e Aggiornamento del sistema operativo e di altri programmi presenti) devono essere configurate in modalità di aggiornamento automatico.

- Le credenziali di accesso possono essere sia manuali che di diversa tipologia (es. mediante certificati digitali): in generale si opterà per modalità di accesso remoto senza l'utilizzo di credenziali manuali

- Nel caso di operatore già in possesso di credenziali di accesso, attenersi esclusivamente ai passi descritti dal paragrafo 3.1

Di seguito si riporta la procedura necessaria per richiedere un accesso VPN

- Nota 1: seguire le indicazioni riportate nella procedura scrivendo agli indirizzi riportati nella procedura e non facendo 'rispondi a tutti'

- Nota 2: come oggetto dell'email inserire: “Richiesta VPN per 'nome Azienda' ” (es: “Richiesta VPN per IBM”)

- Nota 3: IMPORTANTE: a fronte di operatori per i quali è stata precedentemente effettuata la richiesta di autorizzazione VPN ma per i quali non sono più in essere le condizioni necessarie per garantire l'accesso (cambio mansione, interruzione del rapporto di lavoro, ecc.) è OBBLIGATORIO comunicare agli indirizzi email sotto riportati la richiesta di disattivazione VPN, specificando nome, cognome e matricola dell’operatore/degli operatori

in oggetto. Gli stessi indirizzi di posta vanno utilizzati per richiedere eventuali nuove utenze, specificando per ciascuna il set di dati richiesto. Infatti non vanno utilizzate credenziali altrui e non vanno lasciate utenze non più necessarie attive.

2 Attività propedeutiche per la generazione di VPN

A seguito dell'email di richiesta, verrà resa disponibile una VPN SSL basata sulla tecnologia Fortinet.

Come credenziali personali VPN potrà essere necessario inserire un identificativo personale ed una password che verranno forniti. Tali credenziali sono ad uso esclusivamente personale e non devono mai essere cedute ad altri. Occorre inoltre dotarsi di tutti gli accorgimenti necessari affinché non vengano utilizzate da altri (gli accessi verranno registrati a nome dell'utente logico, che dovrà sempre corrispondere alla persona fisica a cui è stato consegnato).
A causa di vincoli tecnologici non è possibile impostare il cambio password dell'utenza utilizzata per la connessione VPN al primo accesso, e verranno fornite istruzioni su come modificarla in autonomia.

Alternativamente potranno essere forniti altri metodi di autenticazione (in tal caso verranno spiegati e verrà fornita assistenza). Tali metodi sono considerati più sicuri dalle linee guida internazionali in tema di sicurezza informatica, ed è per questo che a tendere diverranno la modalità unica di accesso,

Per la predisposizione delle utenze VPN e' necessario che vengano fornite, per ogni persona fisica (le utenze sono strettamente personali come da disposizioni legislative vigenti), le seguenti informazioni:

1. Nome e Cognome
2. Luogo e Data di Nascita
3. Codice Fiscale (il CF non è un dato sensibile in Italia);
4. Scansione leggibile di un documento di identità valido (fronte e retro)
5. Data di scadenza della connessione, corrispondente alla data più prossima tra:
    1. conclusione del rapporto lavorativo con la propria Ditta
    2. conclusione dell'attuale contratto tra ASST e la Ditta
6. Ragione Sociale Ditta
7. Indirizzo Ditta
8. Recapito telefonico

9. Email aziendale
10. Dettagli sistema operativo utilizzato come client per la connessione VPN (Windows/Linux/Mac/Android/altro)
11. Connessioni da autorizzare quando collegati alla VPN (indirizzi IP e servizi che devono essere resi accessibili – ossia porte e relativi protocolli)

Con riferimento al punto 5, laddove sussistono le condizioni di un rinnovo (ossia l'utenza deve essere resa disponibile per un periodo di tempo successivo a quello precedentemente indicato come data di scadenza dell'account, che è obbligatorio specificare) scrivere all'indirizzo email

segreteriaugid@asst-pg23.it

specificando, per ciascun operatore

1. nome e cognome
2. matricola completa di eventuali zeri iniziali
3. nuova data di rinnovo, che deve sempre rispettare la regola prevista al precedente punto 5

Queste informazioni devono essere comunicate, insieme ai riferimenti (nome, cognome, email e/o telefono) del/i referente/i lato ASST con cui la Ditta ha contatti, inviandole, a mezzo email, ai seguenti indirizzi (nessuno escluso):

Destinatari principali:

segreteriaugid@asst-pg23.it
vmolisano@asst-pg23.it
abettinelli@asst-pg23.it
gcrotti@asst-pg23.it

Copia conoscenza:

referente/i lato ASST

Le informazioni sopra elencate dovranno essere comunicate in qualsiasi caso, anche se già fornite in

precedenza.

Una volta ricevute tali informazioni verranno comunicate telefonicamente oppure via email le credenziali di accesso oppure le modalità di accesso alternative da parte dell'ufficio UGID (Ufficio Gestione Identità Digitali c/o ICT).

NOTE IMPORTANTI - Si ribadiscono le seguenti indicazioni:

- La Ditta deve comunicare tempestivamente quando non sussistono più le condizioni necessarie per garantire ad un suo operatore autorizzato l'accesso alla VPN.

- Quando, per qualsiasi ragione, non sussistono più le condizioni tra Ditta e ASST tali da garantire gli accessi VPN in essere, gli stessi verranno revocati da ASST. In tal caso la Ditta non sarà ulteriormente autorizzata ad accedere per nessuna ragione ai sistemi/dati di ASST. Lo stesso vale anche in caso di assenza di esplicita rimozione dei privilegi di accesso lato ASST: in caso di mancanza di condizioni tali da garantire gli accessi VPN in essere la Ditta non deve per nessuna ragione accedere ai sistemi di ASST.

3 Istruzioni per la creazione di una VPN

1 VPN TLS Fortinet

NOTA IMPORTANTE

E' necessario abilitare il protocollo di sicurezza TLS 1.2 e superiori.
Per impostare o anche solo controllare le impostazioni correnti del protocollo TLS sono disponibili numerose indicazioni su Internet diversificate a seconda del sistema operativo utilizzato.

Download ed installazione del programma Forticlient

L'operatore può scaricare il Programma Forticlient per il proprio sistema operativo al seguente link:

https://www.fortinet.com/support/product-downloads#vpn

Qualora il link non fosse attivo (i siti Web spesso vengono modificati) è sufficiente digitare "forticlient download VPN only" su un qualsiasi motore di ricerca e cliccare sul link della pagina dalla quale è possibile scaricare il Programma. E' importante in ogni caso selezionare la versione del Programma Foticlient indicante VPN-only.

Successivamente è necessario installare il Programma scaricato sul proprio dispositivo.

Configurazione del programma Forticlient

Al termine dell'installazione è necessario configurare il Programma Forticlient in modo che possa essere utilizzato per connettersi in VPN.

Al fine di effettuare la configurazione è necessario eseguire il Programma Forticlient (mediante doppio click sull'icona) e cliccare sulla voce "Configure VPN" (il nome potrebbe variare ma farà sempre riferimento alla configurazione) presente sulla schermata principale della finestra del programma.

Inserire i seguenti dati (i nomi dei campi potrebbero essere riportati in italiano e i campi che non vengono menzionati possono essere lasciati vuoti):

- Connection Name: qualsiasi nome identificativo della connessione SSL-VPN , ad esempio “ASST Papa Giovanni XXIII”

- Remote Gateway: 93.55.127.222

- Customize port: mettere il flag sulla casella corrispondente ed inserire il valore 10443

- Client certificate: lasciare il valore “None” (potrebbe essere necessario modificare questo valore – in tal caso verranno fornite opportune istruzioni)

- Authentication: Mettere la spunta su ‘Prompt on login’ e, se presente, ‘Do not Warn Invalid Server Certificate’

Cliccare su 'Save'

Utilizzo connessione VPN

Successivamente alla fase di configurazione è possibile eseguire il Programma Forticlient mediante doppio click sull'icona.

Per effettuare l'autenticazione inserire nei campi corrispondenti Nome Utente e Password che sono state forniti oppure altri metodi che saranno comunicati e spiegati.

2 VPN site-to-site

In specifici casi è prevista la possibilità di implementare una VPN site-to-site. In questi casi è necessario compilare opportuno modulo di richiesta. Scrivere all'indirizzo
segreteriaugid@asst-pg23.it
per richiedere il modulo da compilare.