www.afa.systems
www.majornet.it
+39 800 852 640
contact.us@afasystems.it

MajorGW – WebON/WebOFF: l'autenticazione per accedere al servizio di navigazione Internet

MajorGW è uno dei moduli funzionali delle piattaforme MajorNet e presenta caratteristiche non comuni nel panorama dei gateway di perimetro. Utilizzarle al meglio permette:

- ✔ la riduzione dell'esposizione ad attacchi informatici
- ✔ la decongestione dei collegamenti ad Internet
- ✔ una maggiore attenzione al tempo lavorativo trascorso in navigazione.

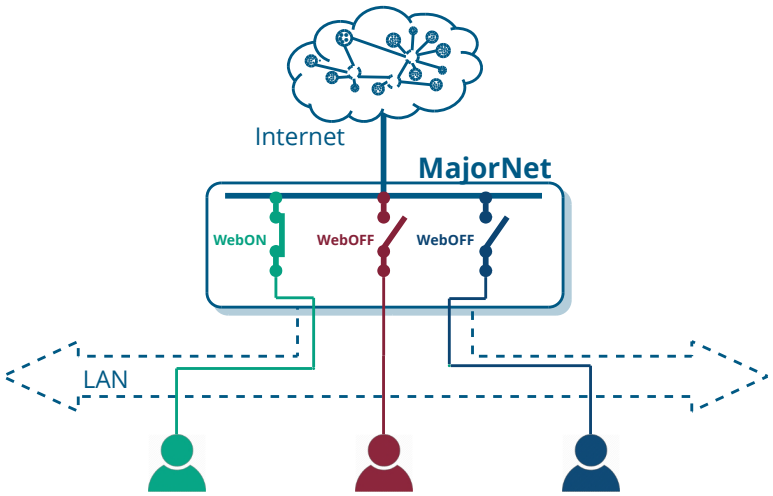
Collegarsi ad Internet

Di continuo dobbiamo autenticarci con password per accedere ai servizi bancari, per effettuare acquisti on-line, per leggere le nostre email. Non siamo abituati invece ad autenticarci per navigare su Internet, come se la navigazione non fosse un servizio critico da proteggere e dal quale derivano dirette responsabilità tanto per l'utente-navigatore quanto per chi gestisce la rete. Entrambe queste figure possono tutelarsi grazie al modulo gateway MajorGW.

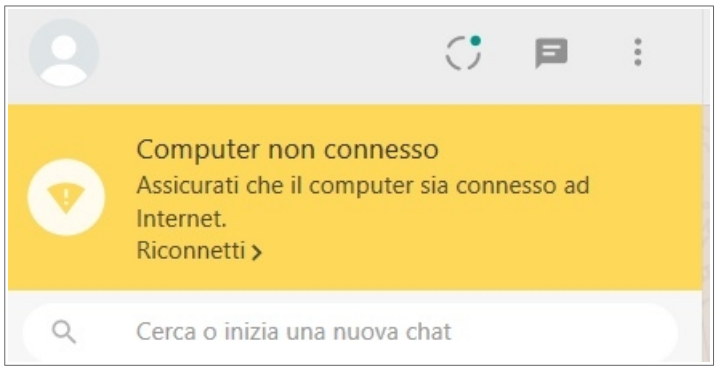
MajorGW è caratterizzato da funzionalità che permettono a ciascun utente di isolare da Internet i suoi dispositivi, pur lasciandoli connessi alla LAN, per utilizzare i servizi interni dell'azienda o dell'ente, ad es. i server, le stampanti, i sistemi di back-up, etc.

Isolandoli i dispositivi interni da Internet, se ne accresce in modo importante la protezione e si riduce il rischio che questi, magari a seguito di un attacco informatico, si trasformino essi stessi in una fonte di attacchi interni, sulle LAN dell'azienda o dell'ente, e di attacchi esterni verso Internet.

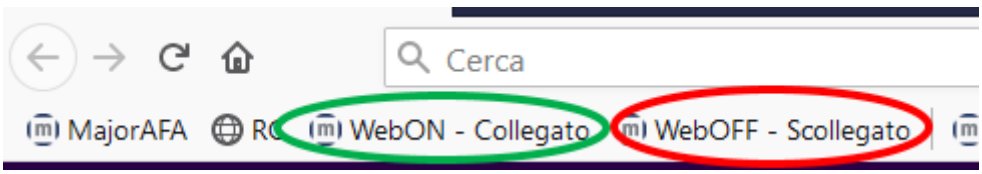
Ciascun utente può azionare il suo interruttore virtuale di collegamento ad Internet, come nella figura che segue.



Quando il tuo dispositivo è scollegato da Internet, nello stato di WebOFF, le app e i programmi (anche quelli che non stai usando!) rilevano la mancanza di accesso ad Internet e segnalano la situazione. Nelle immagini che seguono le segnalazioni generate da Whatsapp su PC Windows.



Gli “interruttori” del collegamento ad Internet possono essere resi facilmente accessibili, utilizzando le funzioni “Segnalibro” che tutti i browser hanno, come nell’esempio che segue:



Il governo dell’accesso ad Internet

Semplificando al massimo, MajorGW permette l’accesso ad Internet ai soli utenti abilitati e dotati di credenziali valide (username e password). Per avviare la propria navigazione, collegando la propria postazione ad Internet, l'utente deve compiere un atto esplicito e volontario, ossia l'azionamento della funzionalità di WebON; simmetricamente, l'utente può scollegare il suo dispositivo da Internet, azionando la funzionalità di WebOFF.

Con MajorGW le attività di navigazione possono essere:

- ✔ concesse a tutti gli utenti, oppure solo ad alcuni di essi, con uno o con più dispositivi contemporaneamente;
- ✔ limitate in tempo di navigazione e/o in traffico scambiato con Internet, con limiti differenziabili per utente;
- ✔ soggette ad ambiti di siti web ammessi, ovvero di siti non ammessi, valutati dinamicamente sulla base del contenuto dei siti web navigati.

Va notato che MajorGW fa riferimento agli utenti e non solo agli indirizzi IP delle postazioni utente, come normalmente avviene nella maggior parte dei gateway e firewall: il collegamento ad Internet avverrà in favore di una postazione client (che ha uno specifico indirizzo IP) solo se esso è stato attivato da un utente abilitato alla navigazione. Se l'utente si trova nello stato di WebOFF, la sua postazione (ad es. il suo PC) non può effettuare nessuno scambio dati verso Internet: risultano bloccati la navigazione via browser, il prelievo, l'invio e la sincronizzazione della posta elettronica, gli aggiornamenti di sistema e soprattutto quegli scambi dati che varie applicazioni attivano a completa insaputa dell'utente. Autenticarsi per navigare su Internet costituisce così l'elemento chiave di un'esperienza nuova e benefica: lavorare scollegato da Internet, senza che le app e i programmi del tuo device possano interagire con server esterni a tua insaputa e fuori dal tuo controllo.

Nello stato di WebOFF stai riducendo l'esposizione a cyberattacchi del tuo device. Anche se viene malauguratamente colpito da virus, il tuo device è messo in condizione di non poter pregiudicare il funzionamento e la "reputazione" dell'intera rete aziendale. Tanti device in WebOFF riducono l'esposizione complessiva ai rischi informatici e le responsabilità connesse. Una policy di "*WebOFF by default*" è una prova concreta di quella *accountability* che il GDPR richiede e una strategia di riduzione del rischio in linea con le indicazioni di molte norme internazionali (ISO 27001, etc.).

Disabilitare la navigazione

Abilitando o meno ciascun utente della tua rete al WebON ottieni l'effetto di abilitarlo o meno a navigare su Internet. Gli utenti non abilitati alla navigazione restano comunque collegati alla rete aziendale per utilizzarne le risorse (server, stampanti, back-up, etc.). La navigazione può essere concessa a tutti gli utenti o solo ad alcuni, limitata individualmente in tempo e/o in traffico. Le azioni di WebON e WebOFF sono registrate e con esse le attività, il tempo e i traffico di navigazione, e sono consultabili attraverso una serie di schermate come quella che segue.

UTENTE	COMPUTER	INDIRIZZO IP	STATO	DW INST	UP INST
[illegible]	local-172-16-0-176	172.16.0.176	On	126,52KB	52,55KB
[illegible]	faure	172.16.16.26	On	301,89KB	4,69KB
[illegible]	local-172-16-0-195	172.16.0.195	On	670,04KB	374,86KB
[illegible]	local-172-16-0-25	172.16.0.25	On	780,59KB	262,91KB
[illegible]	local-172-16-0-18	172.16.0.18	On	458,84KB	37,44KB
[illegible]	local-172-16-0-92	172.16.0.92	On	33,29KB	55,93KB
[illegible]	puccini	172.16.16.19	On	1,87MB	313,41KB
[illegible]	local-172-16-0-96	172.16.0.96	On	14,26MB	571,6KB
[illegible]	local-172-16-0-23	172.16.0.23	Off	0	0
[illegible]	majorafa	10.254.253.1	Off	0	0
[illegible]	amorosa-l2tp	172.19.0.12	AlwaysOn	0	0
[illegible]	backup	172.16.16.210	AlwaysOn	104	180

WebON/WebOFF per lo smart-working

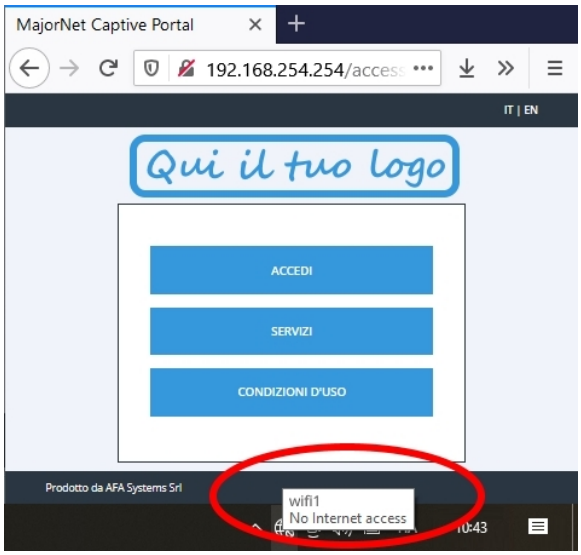
MajorGW viene utilizzato spesso per permettere ai tele-lavoratori di fare accesso alle risorse aziendali tramite Internet in VPN (Virtual Private Network). Anche in questa condizione operativa di smart-working da remoto restano efficaci tutti i benefici, le protezioni e i controlli delle funzioni WebON/WebOFF. Ciò significa in particolare che le postazioni remote, quando scollegate da Internet, non risultano una via aperta ad attacchi informatici esterni, neppure per le reti aziendali e del cloud privato.

Interceptor

Se l'utente inizia a navigare senza aver azionato il WebON, viene ridiretto su una pagina web di benvenuto ("*interceptor*") personalizzabile con loghi e grafica e dinamicamente con informazioni di servizio di varia natura, a seconda che l'organizzazione sia una struttura turistica, un'azienda, una scuola, etc.

Lo stesso utente può eseguire il WebON anche da più dispositivi contemporaneamente. L'utente che vuole scollegarsi da Internet può azionare il WebOFF. In assenza di traffico Internet, dopo un certo tempo la funzione di "*Smart hang-up*" scollega automaticamente l'utente.

Nell'immagine che segue è evidenziata la segnalazione di assenza di accesso da Internet di un PC Windows, con la conseguente ridirezione sulla pagina web di benvenuto.



AutoWebON

Per semplificare le attività dell'utente-navigatore, il WebON può essere automatico, se l'utente è configurato in AutoWebON: dopo il primo WebON esplicito (ad es. al mattino), il dispositivo utilizzato da quell'utente si collegherà automaticamente ad Internet ogni volta che l'utente vuole navigare ed anche quando un programma o un'app accedono a risorse Internet. Così l'utente non deve più comandare il WebON per collegarsi ad Internet, ma mantiene sempre la possibilità di comandare il WebOFF e isolarsi da Internet se lo desidera. Quando il dispositivo abbandona la rete (e il lease DHCP non viene rinnovato) il dispositivo viene scollegato da Internet.

AlwaysINaddress, AlwaysINproto

Puoi rendere accessibili siti e servizi esterni di particolare interesse, anche nello stato di WebOFF.

Per esempio, può essere utile far sì che l'accesso al proprio sito istituzionale o aziendale sia sempre possibile, cioè che agli utenti dell'organizzazione, anche quando sono in WebOFF, possano pervenire le informazioni da questo sito, che verrà inserito nella tabella dei siti AlwaysINaddress (individuati per indirizzo e/o per URL) sempre accessibili. Altri siti sempre accessibili possono essere quelli di particolare interesse per l'organizzazione, che possono essere, ricorrendo ad alcuni "pseudo-esempi" in diversi settori: www.agenziaentrate.gov.it, www.asl-locale.it, www.inps.it, www.la-nostra-banca.it.

In modo analogo può essere utile far sì che, anche per gli utenti in WebOFF, sia sempre possibile ricevere servizi gestiti all'esterno. Prendendo ad esempio la posta elettronica, allora verranno abilitati, nella tabella dei servizi AlwaysINproto, i protocolli email IMAP, SMTP, POP3, permettendo ad ogni utente l'uso dell'email su qualsiasi server email esterno, anche quando l'utente è in WebOFF.

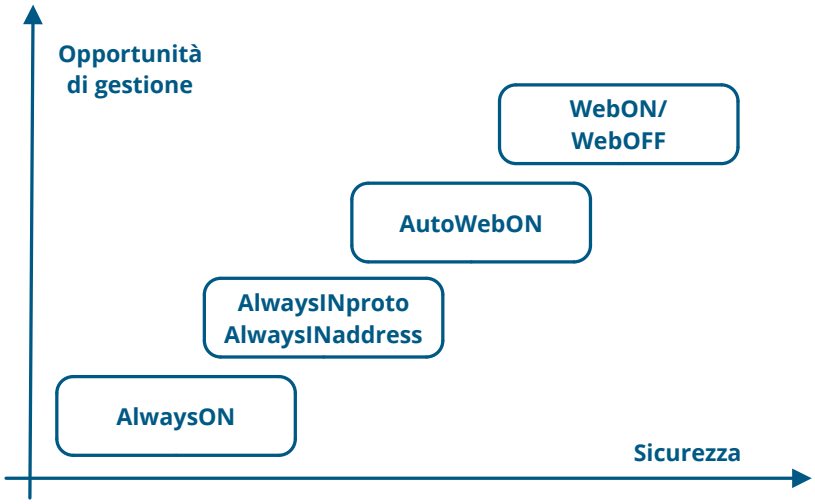
I siti e i servizi esterni configurati in AlwaysINaddress e AlwaysINproto saranno accessibili anche per gli utenti non abilitati alla navigazione Internet e senza limitazioni in tempo e traffico, con qualche riduzione delle possibilità di governarne le attività Internet.

AlwaysON

E' infine possibile abilitare la navigazione di un device in modo permanente ed incondizionato. Per senza richiedere di eseguire il WebON e senza limitazioni di orario, di tempo e di traffico, MajorGW fornisce sempre informazioni sulle attività Internet del device in AlwaysON.

Conclusioni

La condizione di AlwaysON, di fatto l'unica disponibile nei comuni gateway di perimetro. Ad essa, come abbiamo visto, MajorGW aggiunge una serie di possibilità di gestione dell'accesso ad Internet che lo rendono unico. Lo schema seguente le riepiloga, in relazione alla caratteristiche complessive di sicurezza.



Le motivazioni relative alla sicurezza informatica sono importanti e da sole sufficienti per introdurre l'uso delle funzionalità di WebON/WebOFF, magari con l'aiuto di una campagna informativa per gli utenti.

Ma ci sono anche un altro paio di benefici non secondari.

L'accesso ad Internet a seguito di un suo comando, rende l'utente maggiormente consapevole ed attento all'impiego del proprio tempo online, spesso determinandone una riduzione ed incrementando la produttività ed i risultati operativi conseguiti.

Ed ancora, l'eliminazione del traffico Internet "inconsapevole", che avviene cioè indipendentemente dalla volontà dell'utente, determina una riduzione complessiva del traffico sulla linea Internet e la decongestiona, consentendo a tutti una maggior velocità di navigazione.

Il tuo parere è importante

Clicca su uno o più link o scansiona uno o più QR Code per darci il tuo parere anonimo.

Il documento è poco chiaro	Il documento è poco utile	Il documento è poco esauriente	Tienimi informato sulle novità MajorNet
			

MajorNet® è un prodotto di AFA Systems, nato dalla necessità di organizzare la gestione di reti complesse, in maniera più semplice ed efficace, integrando in modo coerente tutti i servizi IP. Piattaforme innovative, testate in migliaia di installazioni di ogni tipo e dimensione.

AFA Systems: un'azienda italiana, focalizzata sulle esigenze dei clienti e collegata ai circuiti internazionali più avanzati delle tecnologie Internet.