

## Rete sotto controllo: se l'azienda è sicura, anche l'investimento è protetto

Sogegross, una delle realtà storiche della Grande Distribuzione italiana, ha scelto le soluzioni di sicurezza Cisco, fornite da Var Group (filiale di Genova), per proteggere la rete dalle potenziali minacce provenienti da accessi non controllati. La gestione centralizzata e automatica della security ora permette all'azienda genovese di utilizzare tempo e risorse del reparto IT per attività focalizzate sul business.

## In breve

### Azienda

Sogegross

### Settore

GDO

### La sfida

- Adeguare i sistemi di sicurezza IT per evitare attacchi e responsabilità legali
- Effettuare il controllo degli accessi di tutti i dispositivi alla rete

### Obiettivi raggiunti

- La rete e l'azienda sono al sicuro da minacce interne ed esterne
- I dipendenti operano in un ambiente protetto
- Ottimizzazione delle procedure di gestione della sicurezza
- Risparmio in termini di tempo per gli utenti e per lo staff IT

Parlando di sicurezza informatica, l'opinione comune è che le principali minacce ad una rete aziendale provengano dall'esterno. Sicuramente Internet e posta elettronica, da sempre, danno non pochi pensieri agli amministratori di rete. L'esperienza insegna però che occorre non abbassare mai la guardia nemmeno contro i pericoli provenienti dall'interno del perimetro aziendale. Può succedere, anche se involontariamente. Per le imprese distribuite sul territorio in cui operano consulenti ed agenti, per esempio, è sufficiente un portatile con un antivirus non aggiornato che si connette alla intranet senza controlli adeguati, e il danno è fatto. In questo scenario, il controllo degli accessi alla rete è più che fondamentale. E solo con una gestione centralizzata dell'intera infrastruttura si può avere la massima visibilità su chi si connette alla rete interna e in che modo. Gli amministratori di rete e gli imprenditori, di conseguenza, possono dedicarsi così alle loro attività principali: sfruttare tecnologia e innovazione per migliorare il business, i primi, e raccoglierne i frutti, i secondi. In che modo? La gamma delle soluzioni Cisco dedicate alla sicurezza intelligente delle reti comprende anche una appliance dedicata al controllo degli accessi. Cisco NAC (Network Admission Control) è una soluzione innovativa che consente la gestione centralizzata e l'applicazione delle policy di sicurezza su tutti i dispositivi che si connettono alla rete aziendale indipendentemente dalla tipologia, modalità di accesso e ubicazione. E proprio su Cisco NAC è caduta la scelta di Sogegross, realtà italiana del settore della GDO, per dotarsi di uno strumento di sicurezza proattivo in grado di proteggere in modo automatico tutte le porte di accesso alla rete aziendale, a seguito di un episodio di minaccia dall'interno che aveva reso necessario un nuovo approccio alla sicurezza di rete.

Sogegross nasce nel 1920 a Genova come semplice negozio di drogheria. Da allora molte cose sono cambiate, se l'antico esercizio è diventato un Gruppo attivo nella maggior parte delle regioni del centro-nord Italia, con 2.400 addetti, 5 canali, più di 200 punti vendita e una presenza capillare in tutte le tipologie di canale distributivo. Il nuovo corso ha origine nel 1970, anno in cui

nasce il primo Cash & Carry che dà l'avvio ad una fase di costante sviluppo. Sogegross in poco più di 30 anni diviene così una tra le prime 10 realtà italiane nel settore della Distribuzione Moderna. Oltre ad essere presente sul territorio con punti vendita tradizionali (Cash & Carry, supermercati e discount alimentari), il Gruppo ha sviluppato l'innovativo settore della spesa on line con il lancio del sito [www.basko.it](http://www.basko.it) e la successiva acquisizione di [www.esperya.com](http://www.esperya.com), il negozio virtuale di enogastronomia italiana più frequentato in Europa. Ad oggi Sogegross comprende anche due Centri Distributivi di Serravalle Scrivia e Tortona, in provincia di Alessandria, che insieme a quelli ubicati presso le sedi di Genova Bolzaneto e di Genova Campi movimentano oltre 65.000 tonnellate all'anno di prodotti freschi e più di 33.000.000 di colli di prodotti confezionati.

Presso Sogegross, una parte del lavoro del settore Sistemi Informativi (e non solo) viene svolta da consulenti esterni, che hanno necessità di utilizzare strumenti e risorse presenti sulla rete aziendale, o comunque di collaborare con il personale del Gruppo via intranet. Ma una rete a cui accedono dispositivi non configurati secondo standard definiti dall'organizzazione può essere soggetta a pericoli, come sottolinea **Marco Staiti**, della Direzione Sistemi Informativi. *“Purtroppo in passato si è verificato un attacco virale involontario, propagatosi dal computer di un nostro consulente. Il virus si è diffuso velocemente andando a bloccare tutti i sistemi informativi e tutti i client connessi sia in sede che presso le filiali sul territorio”*. È facile immaginare il danno in termini di tempo di indisponibilità di rete e di bonifica dell'infrastruttura. In una azienda moderna, l'inattività della componente di networking equivale ad un fermo del business sotto tutti gli aspetti. *“L'incidente ci ha fatto capire quanto fosse importante avere una adeguata struttura di sicurezza interna, un aspetto che non deve essere secondario alla protezione dalle minacce provenienti dall'esterno”*.

Con il supporto di Var Group, system integrator “partner Cisco” specializzato anche in soluzioni di sicurezza in ambito ICT, il team IT di Sogegross ha focalizzato la necessità di un sistema a controllo degli accessi e ha scelto la più efficace appliance

sul mercato, ovvero Cisco NAC. *“Il nostro obiettivo era di riuscire a controllare tutti i dispositivi che si connettono alla rete, quindi monitorare tutte le porte libere tramite le quali consulenti o utenti guest accedono all’ambiente IT”*. Tramite Cisco NAC, a seguito di ogni accesso alla rete e all’assegnazione di un nuovo indirizzo IP, è possibile attuare in modo centralizzato e automatico un controllo e una verifica sul dispositivo connesso, attraverso l’applicazione di policy personalizzabili stabilite secondo le esigenze di ogni azienda. *“NAC verifica immediatamente che l’utente che si è connesso abbia un software antivirus installato, ne controlla la versione ed esegue un check dello stato degli aggiornamenti del sistema operativo. In casi sospetti, per esempio se il PC è privo degli ultimi update di Windows o dell’antivirus, il sistema blocca l’utente e inibisce l’accesso a ogni settore della rete”*.

Dall’implementazione di Cisco NAC, i vantaggi ottenuti sono numerosi. La sicurezza dell’azienda e degli utenti, in primis. Da una parte, la certezza per i dipendenti di poter operare in un ambiente protetto, dall’altra i responsabili IT e i vertici dell’azienda stessa possono contare su una soluzione che mette Sogegross al riparo anche dalle responsabilità legali che gli attacchi alla sicurezza di rete e alla privacy dei dati possono causare, per non parlare per i costi che ne derivano. Non solo: alla base del bilancio positivo c’è anche l’ottimizzazione delle procedure di gestione della sicurezza e il risparmio in termini di tempo per gli utenti e per lo staff IT. *“La procedura standard precedente all’introduzione di Cisco NAC”*, aggiunge Staiti, *“coinvolgeva le risorse IT per numerose operazioni che impegnavano me ed i miei colleghi, sottraendo tempo alle attività core business. Ogni consulente ci interpellava per il collegamento alla rete e per la configurazione del PC, la nostra presenza sul posto era indispensabile”*. Non tutte le porte erano infatti abilitate di default al collegamento in rete, il che implicava un dispendio di forze per azioni di controllo. *“Oggi, al contrario, tutto il processo si svolge in modo automatico. Le porte disponibili sono sotto il controllo di Cisco NAC, e ad ogni nuovo accesso viene assegnato un nuovo indirizzo IP. La connessione alla rete è oltremodo facilitata: ogni utente esterno è in grado di procedere in autonomia senza bisogno del nostro aiuto”*.

Secondo Staiti, ora i Sistemi Informativi impiegano il 40% di tempo in meno nelle operazioni di gestione della sicurezza grazie alle funzionalità di Cisco NAC. Tempo prezioso che lo staff IT può finalmente dedicare allo svolgimento di attività finalizzate al

business dell’azienda, per un generale miglioramento della produttività. L’aver scelto una appliance e una architettura ridondata offre a Sogegross la massima affidabilità, con prestazioni e livello di gestione senza confronti e ulteriori risparmi di tempo. *“Non stiamo parlando di un software, come un antivirus, che necessita di upgrade e aggiornamenti. Una appliance ha il vantaggio di essere un dispositivo ad hoc, richiede minore impegno di gestione e ci consente di dedicarci ad altro”*. Un punto di vista confermato da Paolo De Seta, Territory Business Manager di Cisco. *“Le aziende come Sogegross possono sfruttare i molteplici vantaggi generati dalle soluzioni di sicurezza Cisco. Da una parte possono mettere le risorse e beni aziendali al sicuro da minacce interne ed esterne, dall’altra liberano il dipartimento IT dalle incombenze associate alla fornitura di accessi alle reti aziendali, aiutandolo a non diventare un collo di bottiglia per le richieste di intervento”*.

A quasi due anni dall’implementazione, forti dell’esperienza positiva provata grazie alla consulenza tecnologica di Var Group e al valore delle soluzioni Cisco, Staiti e il suo team stanno già lavorando per dotare di adeguati sistemi di controllo anche i consulenti che accedono alla rete da remoto, il che estenderà in modo pervasivo la protezione interna a 360 gradi su tutta la rete. Un passo che conferma la fiducia di Sogegross verso Cisco e il supporto ottenuto dal partner. *“Var Group collabora con noi da parecchi anni, è il nostro fornitore unico in ambito IT e assistenza sistemistica, c’è un rapporto di fiducia che va oltre l’aspetto commerciale. Quanto a Cisco, scegliendo le sue soluzioni andiamo sul sicuro. Potremmo anche valutare soluzioni di altri produttori, ma l’assistenza successiva all’acquisto che ci mette a disposizione Cisco, supportata dall’esperienza e la competenza del suo personale tecnico, fa sempre la differenza”*.



## Link utili

**Cisco**  
[www.cisco.com/it](http://www.cisco.com/it)

**Sogegross**  
[www.sogegross.it](http://www.sogegross.it)

**Soluzioni Cisco per la sicurezza IT**  
[www.cisco.com/web/IT/solutions/sicurezza/security\\_index.html](http://www.cisco.com/web/IT/solutions/sicurezza/security_index.html)

**Var Group**  
[www.vargroup.it](http://www.vargroup.it)



**Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 001 408 526-4000

**Sede italiana**  
Cisco Systems Italy  
Via Torri Bianche, 8  
20059 Vimercate (MI)  
[www.cisco.com/it](http://www.cisco.com/it)  
Numero verde: 800 782648  
Fax: 039 6295299

**Filiale di Roma**  
Cisco Systems Italy  
Via del Serafico, 200  
00142 Roma  
Numero verde: 800 782648  
Fax: 06 51645001

Le filiali Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito Cisco all'indirizzo: [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

© Giugno 2010 Cisco Systems, Inc. Tutti i diritti riservati. Il logo Cisco e Welcome to the Human Network sono marchi registrati di Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn è un service mark di Cisco Systems, Inc.; e Access Registrar, Aironet, Catalyst, CCDA, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, il logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, il logo Cisco Systems, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, il logo iQ, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, e TransPath sono marchi registrati di Cisco Systems, Inc. e/o di società partner negli Stati Uniti e in determinati altri paesi.

Tutti gli altri marchi o marchi registrati in questo documento o sul sito Web sono proprietà delle rispettive aziende. L'utilizzo della parola partner non implica una relazione di partnership tra Cisco e qualsiasi altra azienda.