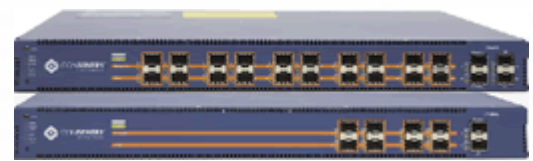


Sicurezza della LAN. NAC + Role-based LAN Segmentation.

Secure Switching.

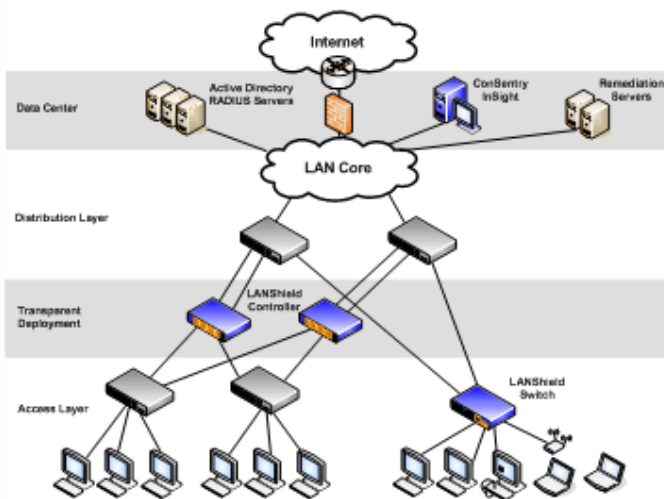
ConSentry Networks propone soluzioni di secure switching che consentono il controllo di ogni utente e di ogni porta sulla LAN. Le piattaforme LANShield—LANShield Controller e LANShield Switch— sono devices specificatamente costruiti, e basati su processori disegnati su misura, per permettere il controllo di ogni flusso di dati. Con ConSentry, l'IT è in grado di controllare chi può accedere alla LAN, monitorare e limitare quello che l'utente può fare sulla LAN e prevenire minacce in grado di compromettere dati ed interrompere servizi di rete.



LANShield Controller



LANShield Switch



Network Access Control.

La piattaforma ConSentry LANShield fornisce funzionalità di network access control necessarie per la sicurezza della LAN, potendola inserire direttamente nell'infrastruttura con LANShield Switch e/o LANShield Controller. Il Controller è un appliance a 4 o 10 porte che aggrega gli uplinks dello switch di core con quelli di accesso. Lo Switch è invece un vero e proprio switch con funzionalità di NAC disponibile a 24 o 48 porte. ConSentry InSight command center permette di avere una piena visibilità della LAN e di creare e distribuire le policy per i prodotti LANShield.

Sicurezza della LAN.

La famiglia di prodotti LANShield consente di usufruire di un set completo di funzionalità di network access control necessarie alla protezione completa degli asset, quali:

Network Admission Control (NAC) – Autenticazione e posture check (verifica dello stato e della conformità alle policy del device) per l'ammissione dell'utente alla rete LAN.

Visibilità – Informazioni su eventi e anomalie, relative allo username, a Livello 7 sui protocolli (es.: nomi dei files, URLs).

Controllo basato sull' Identità – controllo dell'accesso tramite regole per limitare l'attività degli utenti sulla LAN.

Controllo delle minacce – individuazione e blocco del propagarsi di worms o altri malware per prevenire ed evitare che la rete divenga inutilizzabile.



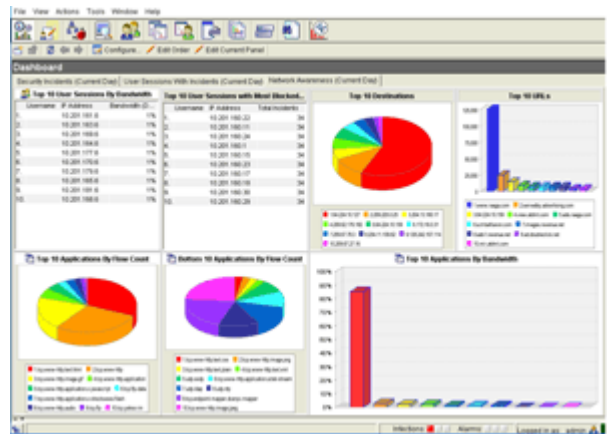
Network Admission Control.

ConSentry supporta il NAC appoggiandosi ai server esistenti di autenticazione e identità (Radius, AD, etc) e sulla propria infrastruttura di integrity check. Ove richiesto, LANShield Switch e LANShield Controller possono eseguire l'autenticazione e l'host posture check senza la necessità dell' 802.1x o di un agent installato sui client.



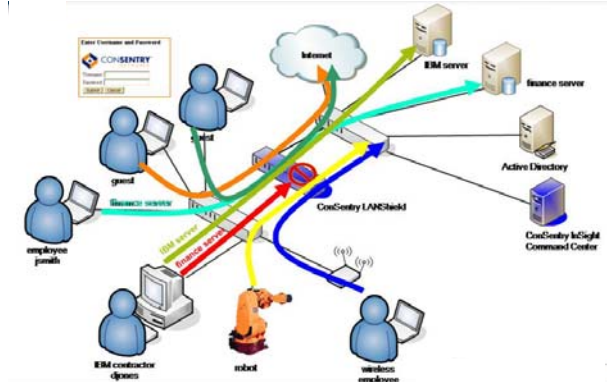
Visibilità Completa.

LANShield Switch e LANShield Controller forniscono una in-depth packet inspection con la piena decodifica dell'applicazione a livello 7. In questo modo possono distinguere tra applicazioni che utilizzano la stessa porta a livello 4 o che tentano di mascherarsi usando un numero di porta tipicamente non associato a quella applicazione. LANShield può filtrare il traffico in base al contenuto del pacchetto e attraverso l'associazione user name a IP e MAC address può tracciare il traffico LAN per utente individuale, gruppi di utenti, applicazione, host, protocollo, porte L4, transazioni o accesso a files. Il grado di visibilità facilita eventuali reazioni a possibili incidenti.



Controllo basato sull'Identità.

LANShield Switch e LANShield Controller sono in grado di applicare controlli che limitano l'accesso dell'utente alle risorse di rete, attraverso la definizione di policy relative al proprio ruolo all'interno dell'organizzazione. Questo controllo basato sull'identità, verrà applicato universalmente ed indifferentemente rispetto al luogo ed alla modalità di accesso dell'utente alla rete.



Controllo delle minacce.

La famiglia dei prodotti LANShield offrono la protezione contro minacce conosciute e non, fornendo un accurata individuazione con blocco granulare di una transazione, come ad esempio per URL. In presenza di un malware LANShield è quindi in grado di bloccare una transazione per utente o per applicazione, lasciando inalterate le transazioni lecite. Per migliorare la sicurezza di applicazioni VoIP ed evitare che le stampanti diventino un veicolo per un attacco, ConSentry può limitare i protocolli che stampanti, telefoni e altri device possono eseguire e limitare la destinazione ad una determinata rete.

