molto più di un

NETWORK ACCESS CONTROL

VISIBILITA´
CONTROLLO
SICUREZZA

- CAPTIVE PORTAL
- CLUSTER
- ENDPOINT
- FINGERPRINTING
- IDENTIFICAZIONE DEI DISPOSITIVI
- GESTIONE CON SENSORI
- VLAN-MANAGER
- PROTEZIONE DEGLI ACCESSI

ARP-GUARD è la nostra collaudata soluzione Network Access Control (NAC) che, a differenza di complesse e costose applicazioni di rete, può facilmente essere realizzata anche in reti eterogenee e di grandi dimensioni. Il sistema identifica in modo veloce e sicuro sia le apparecchiature conosciute che quelle sconosciute, indipendentemente dal produttore o dalla tecnologia, prima che ottengano l'accesso alla rete. Oltre alla pura protezione degli accessi, la soluzione raggruppa a livello centrale anche le informazioni rilevanti per la sicurezza, rileva e segnala le anomalie nella rete e le corregge prontamente.

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

WWW.ARP-GUARD.COM

LA SOLUZIONE ARP-GUARD IN DETTAGLIO

RILEVAMENTO E INVENTARIO DEI DISPOSITIVI

ARP-GUARD comunica con l'intera infrastruttura di rete e rileva tutti i sistemi ivi presenti nel giro di pochissimo tempo. Ogni Endpoint diventa visibile e le fonti di malfunzionamento possono essere rapidamente localizzate ed eliminate. In aggiunta, la soluzione presenta l'intera architettura in una topologia grafica. Questo non solo facilita la pianificazione della rete, ma permette la trasparenza richiesta nell'ambito di audit e verifiche.

PROTEZIONE DEGLI ACCESSI

Il controllo centrale e la regolazione di tutti gli accessi alla rete forniscono un controllo omnicomprensivo. Le apparecchiature sconosciute vengono rilevate e segnalate in tempo reale. L'identificazione univoca di un dispositivo è seguita dalla relativa applicazione dei processi predefiniti. Dalla disattivazione immediata di una porta al trasferimento in una speciale Virtual Local Area Network (VLAN), qualsiasi azione desiderata può essere definita e gestita per l'intera rete attraverso l'assegnazione di criteri specifici.

SEGMENTAZIONE DELLA RETE ATTRAVERSO LA GESTIONE DELLE VLAN

Con la gestione delle VLAN, la segmentazione della rete può essere facilmente attuata e comodamente gestita. Le aree sensibili sono in tal modo particolarmente protette, le aree pubbliche sono ben separate dalle aree interne e gli ospiti e i fornitori di servizi dispongono solo di un accesso dedicato. Anziché configurare manualmente le singole porte dello switch, l'assegnazione alla VLAN è automatizzata attraverso l'attuazione dei criteri predefiniti. I dipendenti che si spostano, viaggiano o lavorano in altre sedi portano sempre con sé il proprio "ambiente IT".

FINGERPRINTING

La combinazione di diversi metodi di autenticazione, come RADIUS basato su MAC e 802.1X, fornisce sicurezza e flessibilità. Noi completiamo questi metodi con ARP-GUARD Fingerprinting. Fingerprinting acquisisce diverse caratteristiche, come certificati e chiavi crittografiche, per identificare veramente in modo univoco ogni dispositivo.

ARCHITETTURA DI GESTIONE A SENSORI

Grazie alla particolare architettura di gestione con sensori, ARP-GUARD è adatta ad ambienti multi-sede ed è enormemente scalabile. Il ricorso ad un sistema a sensori permette l'integrazione efficace di qualsiasi numero di sedi aziendali. La soluzione Enterprise permette l'amministrazione di grandi ambienti di rete decentralizzati. Un motore centrale di regole gestisce tutta la rete ad "ombrello", in maniera semplice e automatizzata. Utenti, ruoli, diritti e policies vengono di conseguenza sincronizzati. Tuttavia, i sensori possono essere utilizzati anche in modo decentralizzato.

COMPONENTI AGGIUNTIVI

CAPTIVE PORTAL - ACCESSI OSPITI & BYOD

Il componente aggiuntivo Captive Portal regola l'accesso alla rete di dispositivi di ospiti e di terzi, come ad esempio smartphone o notebook. In ogni ambiente è possibile definire accessi di rete mirati per apparecchiature di terze parti. Tali accessi sono controllati in ogni momento da un sistema di criteri firewall-dinamici anche tra sedi diverse grazie all'architettura di gestione dei sensori. In tal modo il Bring Your Own Device (BYOD) è facile da realizzare e i dispositivi privati ricevono solo un accesso esplicitamente autorizzato.

INTEGRITÀ DI TUTTI GLI ENDPOINT

La funzione ARP-GUARD Endpoint fornisce un prezioso supporto per attuare i requisiti di conformità. Durante l'autenticazione viene controllato se gli endpoint aderiscono alle linee guida di sicurezza e se sono conformi in merito ai dettagli rilevanti per la sicurezza, come ad esempio lo stato, l'antivirus o il livello di patch del sistema operativo. Se le linee guida non sono soddisfatte, il dispositivo viene isolato e può essere aggiornato in una VLAN di quarantena. Solo dopo il controllo e l'eventuale aggiornamento le apparecchiature ricevono l'accesso alla rete.

CLUSTER: ALTA DISPONIBILITÀ PER AREE IT CRITICHE

Il componente aggiuntivo Cluster permette la replica dei server con semplici strumenti software e hardware, al fine di aumentare affidabilità e scalabilità in ambienti IT critici.

ARP-GUARD IN SINTESI

- Rilevamento e inventario delle apparecchiature
- Controllo centralizzato e sorveglianza degli accessi alla rete
- Definizione centrale e applicazione delle linee guida in tempo reale
- Segmentazione della rete
- Integrità della rete LAN/WLAN fino agli Endpoint
- Fingerprinting per l'identificazione univoca dei dispositivi
- Controllo di conformità degli Endpoint
- Regolazione degli accessi per gli ospiti e BYOD
- Riduzione delle attività di amministrazione IT attraverso l'automazione
- Indipendente dai produttori e dalle tecnologie di rete in uso
- Supporto di ISO/IEC 27001, DIN EN 80001-1, PCI/DDS

VALORI AGGIUNTI

SEMPLICE IMPLEMENTAZIONE

Già con l´installazione di base si raggiunge un livello di sicurezza decisamente elevato, che può essere ulteriormente ampliato passo dopo passo. L'integrazione nell'infrastruttura esistente avviene perfettamente e senza problemi, senza bisogno di modifiche o ulteriori investimenti.

MESSA IN SERVIZIO

La soluzione ARP-GUARD è fornita sia attraverso Appliance virtuali che fisici; con un'installazione cluster, sussiste la possibilità di una implementazione mista. Inoltre, i sensori possono anche essere installati direttamente sui server dell'azienda.

PUNTI DI FORZA INTERSETTORIALI

ARP-GUARD viene utilizzato in tutti gli ambiti. Oltre all'industria, al commercio, alla sanità, alle autorità pubbliche, all'istruzione e alla ricerca, la soluzione è decisiva nel settore finanziario, settore molto sensibile ai temi legati alla sicurezza. La flessibilità, l'architettura e la funzionalità di ARP-GUARD sono ideali per le infrastrutture critiche (KRITIS). La conformità ai requisiti di sicurezza di ISO 27001 e DIN EN 80001-1, PCI/DSS e la certificazione sulla base della protezione di base IT sono per noi una cosa ovvia.

MIX DI METODI PER MAGGIORE SICUREZZA E FLESSIBILITÀ

ARP-GUARD copre l'intera gamma di opzioni di autenticazione. La versione 4.0 realizza una perfetta simbiosi di tali opzioni, frutto dell'adozione di innovative strategie di sviluppo. ARP-GUARD permette il funzionamento misto di SNMP, RADIUS basato su MAC e 802.1X con lo stesso set di funzioni. Anche una migrazione successiva da SNMP a 802.1X è facile da realizzare.

SERVIZIO E SUPPORTO

I nostri partner qualificati ed esperti di ARP-GUARD saranno lieti di assistervi in tutti gli aspetti di supporto al prodotto.
www.arp-guard.com/kontakt/vertriebspartner

In aggiunta, potrete anche beneficiare delle nostre ampie offerte di servizio: Software-Subscription (accesso a tutte le Release, aggiornamenti e nuove versioni), supporto di terzo livello (supporto del produttore per l'ottimizzazione e l'adattamento specifico al cliente), formazione tecnica.

SPECIFICHE

Piattaforme di virtualizzazione

Gli Appliance virtuali sono supportati su

- VMware
- Microsoft Hyper-V
- KVM

Sistemi operativi supportati

- Linux, Red Hat
- DOMOS
- CentOS
- Microsoft (Sensoren)

Metodi di autenticazione

- MAC-based RADIUS
- EAP
- SNMP
- 802.1X

Protocolli

- RADIUS
- SNMP
- SSH
- Telnet
- DHCP
- LDAP
- HTTPS
- Kerberos
- WMI

Browser supportati

- Google Chrome
- Mozilla Firefox
- Safari
- Microsoft Internet Explorer
- Microsoft Edge