«Secure Access Switches»

für eine netzwerkweite IT-Security

Dank der nahtlosen Verknüpfung der «Secure Access Switches» der FortiSwitch-D-Serie mit der zentralen IT-Security-Instanz FortiGate ermöglicht Fortinet ein konsolidiertes Sicherheitsmanagement bis auf Switch-Ebene.

Ob KMU, Branch-Office oder dezentral organisierte Unternehmen mit kleineren Niederlassungen: Dank den «Secure Access Switches» der FortiSwitch-D-Serie erhalten sicherheitsbewusste Unternehmen eine leistungsfähige Switch-Familie, die sich nahtlos in die bestehende Firewall- und Secure-WLAN-Infrastruktur von Fortinet einbinden lässt und punkto integrale IT-Sicherheit einen neuen Standard setzt. Kern der Lösung bildet die zentrale Steuerung sämtlicher eingebundener Switches durch die «Next Generation Firewall»-Appliance FortiGate. Dabei wird das gesamte Management der auf Fortinet basierenden Switches durch die zentrale Firewall konsolidiert. Dies vereinfacht das Handling enorm und steigert die Gesamtsicherheit im Vergleich zu heterogenen Gebilden markant.

Übergreifende IT-Security

Das Konzept der nahtlosen Einbindung der «Secure Access Switches» in die FortiGate Security Appliance – die Management-Kommunikation erfolgt über CAPWAP-Protokoll-basierte Tunnel – entspricht dem Bedürfnis, unterschiedlichen Usern und Benutzergruppen (interne Mitarbeitende, Partner, Gäste) hochgradig gesicherte Zugänge zu individuell freigegebenen Daten, Applikationen und/oder Services zu gewähren. Dies unabhängig vom verwendeten Device, von Zugangsort und physischer Zugangsart (kabelgebunden oder via WLAN). So lassen sich unter anderem dedizierte Security-Zonen definieren – etwa für Gäste –, die dank der zentralen Konfiguration zugangsübergreifend Gültigkeit haben. Wird ein Device mit einem FortiSwitch-Port verbunden, erfolgt die Überprüfung der Zugangskomponente sowie eine Authentifizierung des Users. Hat sich dieser mit seinen Zugangsdaten erfolgreich eingeloggt, erhält er gemäss vordefinierten Policies Zugang zu den freigegebenen Ressourcen. Dabei behält die zentrale Security-Instanz stets die Kontrolle darüber, welche Devices und User sich wo und wann im Netz befinden.

Besonders erwähnenswert ist die optionale Einbindung der Authentisierungslösung FortiAuthenticator von Fortinet. Diese dient der sicheren User-Authentifizierung (Überprüfung der Echtheit der berechtigten Person) und User-Autorisierung (Freigabe von Anwendungen gemäss individuell vergebenen Rechten) über das gesamte Firmennetzwerk (NAC 802.1x).

Leistungsstark

Die «Secure Access Switches» von Fortinet sind in unterschiedlichen Ausbaustufen erhältlich. Sie weisen lediglich 1HE auf, unterstützen 8 bis 48 Ports und sind in POE-Ausführungen (Power over Ethernet) verfügbar. Alle Modelle bieten die Möglichkeit, virtuelle LANs mit VLAN-spezifischen Security-Policies zu bilden. Diese (Daten-)Segmentierung unterstützt die Konvergenz von Voice, Daten und WLAN und adressiert weitreichende Compliance-Anforderungen hinsichtlich «Data Separation». Wichtig: Werden von einem VLAN zum anderen Daten übertragen, erfolgt das Routing über die zentrale Security-Instanz FortiGate von Fortinet, was zu einem Höchstmass an Sicherheit führt. Der Einsatz der ausgesprochen performanten, hardwarebeschleunigten FortiGate-Appliances als «Internal Segmentation Firewalls» macht diese integrale «Secure Access Switch»-Architektur möglich.

FortiSwitch-Leistungsmerkmale – ein Auszug:

Mit den «Secure Access Switches» der FortiSwitch-D-Serie revolutioniert Fortinet den IT-Security-Markt.

- Performante «Secure Access Switches» mit 8 bis 48 Ports; auch in POE-(Power over Ethernet-)Ausführungen erhältlich
- Nahtlose Integration in die zentrale Security-Instanz FortiGate von Fortinet; konsolidiertes Security-Management über das gesamte Netzwerk
- Übergreifende User-Authentifizierung und -Autorisierung mit Freigabe von Ressourcen gemäss vorgegebenen Rechten (NAC 802.1x) – inkl. sichere Einbindung von Gästen
- Netzwerkweite Identifikation von Devices und Usern – unabhängig von Zugangskomponenten, -ort und -art (LAN, WLAN, mobile Devices …)
- Bildung von gemeinsamen VLAN- und WLAN-Zonen
- Geschützter Zugang zu dedizierten Netzwerk-Ports – abhängig von definierten Rechten
- Unterstützung konvergenter Umgebungen (Sprache, Daten, WLAN-Traffic)

BOLL
IT Security Distribution

BOLL ENGINEERING AG

Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60, info@boll.ch
www.boll.ch