Forcepoint

Sintesi della soluzione

Forcepoint Next Generation Firewall con Microsoft Azure

Il firewall di fascia enterprise più sicuro ed efficiente, a gestione centralizzata, sempre attivo e vigile

Sfida

- Aziende e organizzazioni devono proteggere i loro ambienti cloud e ibridi con lo stesso livello di sicurezza che avevano nelle tradizionali infrastrutture on-premise
- Lo sviluppo e la manutenzione di un'infrastruttura cloud o ibrida sicura possono essere costosi e tecnicamente complessi
- La conformità alle normative richiede molto impegno e può essere tecnicamente complessa

Soluzione

- Forcepoint Next Generation Firewall offre una soluzione incentrata sul software studiata per offrire il massimo della sicurezza con costi e complessità ridotti al minimo
- Con Forcepoint Security Management Center (SMC) i team possono gestire migliaia di firewall, snellire i processi e ottenere una visibilità ineguagliata con controlli granulari
- La nostra soluzione riduce il lavoro necessario per raggiungere la conformità, in quanto offre policy già pronte, che aiutano a garantire la conformità alle norme nelle reti sia fisiche che virtuali, oltre ad agevolare l'accesso ai report di controllo

Risultato

- Massima sicurezza in ambienti cloud e ibridi e minima complessità
- Risposta accelerata agli incidenti
- Ottimizzazione di conformità alle normative, implementazione e gestione
- Minore costo totale di proprietà (TCO) per la sicurezza e l'infrastruttura di rete

Forcepoint Next Generation Firewall collega e protegge reti aziendali distribuite e complesse. Distribuzioni elastiche zero-touch e un approccio Zero Trust alla sicurezza di rete garantiscono tutta l'efficienza, l'affidabilità e la sicurezza efficace che ti occorrono per difendere il tuo perimetro.

Scelte da migliaia di clienti in tutto il mondo e disponibili tramite Microsoft Azure Marketplace, le soluzioni di sicurezza di rete Forcepoint permettono alle imprese di risolvere le loro criticità in modo efficiente e conveniente, aiutandole a prevenire le violazioni.

Sicurezza Forcepoint per ambienti cloud pubblici

I servizi basati su cloud e le distribuzioni virtuali stanno trasformando le aziende di ogni tipo e dimensione. Le apparecchiature hardware tradizionali stanno scomparendo rapidamente dalle sedi locali perché le organizzazioni hanno bisogno di maggiore efficienza, agilità e controllo dei costi, senza oneri amministrativi e di manutenzione. Per aiutare i nostri clienti a restare competitivi, Forcepoint ha studiato soluzioni per la sicurezza di rete strategiche incentrate sul software: in pratica potrai portarle con te quando ti sposterai nel cloud. La diffusa adozione delle architetture cloud aumenta le responsabilità che gravano sui professionisti della sicurezza e sui responsabili IT, chiamati a garantire che questi nuovi ambienti siano sicuri tanto quanto i precedenti ambienti fisici.

Forcepoint Next Generation Firewall offre soluzioni incentrate sul software, studiate per offrire il massimo della sicurezza con costi e complessità ridotti al minimo. Security Management Center (SMC) di Forcepoint è una piattaforma unificata che offre visibilità e controllo senza confronti e applicazione uniforme delle policy, per aiutare a garantire la conformità alle normative in ambienti fisici, virtuali e cloud.

Sicurezza del cloud di Microsoft Azure

Per proteggere gli ambienti cloud, Forcepoint introduce in Azure la sua tecnologia firewall di nuova generazione, con caratteristiche di scalabilità ed efficienza comprovate e solide funzionalità di protezione. Amplia facilmente e in sicurezza la rete della tua organizzazione, dai data center e dal perimetro di rete fino alle filiali e alle sedi remote, nell'ambiente cloud di Azure tramite un gateway VPN (Virtual Private Network) sicuro. La nostra gestione centralizzata ti consente di creare e distribuire le policy velocemente e in modo omogeneo in tutti i tuoi sistemi. Potrai vedere rapidamente nel dettaglio che cosa succede sia nel tuo ambiente Azure sia sulla tua rete fisica.

I clienti che passano a Forcepoint Next Generation Firewall segnalano un calo dell'86% negli attacchi informatici, un alleggerimento del 53% (in termini di tempo) del carico di lavoro che grava sull'IT e una riduzione del 70% nelle attività di manutenzione programmata.

Massima sicurezza, minima complessità

L'architettura incentrata sul software delle soluzioni di sicurezza di Forcepoint, come la protezione dalle minacce avanzate, l'ispezione approfondita dei pacchetti e il controllo a livello di applicazione, è studiata per facilitare la distribuzione elastica in ambiente locale, virtuale o cloud. I controlli granulari di protocolli, applicazioni e utenti permettono ai team di sicurezza di sfruttare appieno la potenza dell'automazione per ridurre le complessità e il tempo da dedicare a ordinarie attività di sicurezza di base. L'approccio defense-in-depth integrato e completo di Forcepoint è personalizzabile in base alla specifiche esigenze di ogni utente, luogo o asset e include uno o più firewall, VPN, IPS e protezione con URL Filtering. Il nostro Next Generation Firewall offre tutte le funzionalità tipiche di un'appliance hardware avanzata, inclusi ispezione stateful, controllo granulare delle policy e degli accessi e connessioni ISP ridondanti, ma senza l'ingombro fisico.

Visibilità e controllo in tempo reale

Diversamente dalle console di gestione tradizionali, Forcepoint Next Generation Firewall offre visibilità e controllo completi sul flusso del traffico negli ambienti cloud e virtuali. Il successo del nostro SMC deriva dalle sue funzionalità di reportistica veloce e failover automatizzato, che avvisano gli amministratori di imminenti malfunzionamenti di un sistema e prendono automaticamente decisioni in base a regole preconfigurate, in modo da evitare interruzioni nell'esperienza degli utenti. Puoi gestire qualsiasi numero o combinazione di cluster o dispositivi Forcepoint fisici o virtuali, nonché le versioni software in esecuzione su hardware x86 standard. SMC rafforza anche la sicurezza dei sistemi virtuali tramite un dashboard per il monitoraggio olistico con controlli granulari e visibilità su tutto lo stack di applicazioni.

Semplifica la conformità alle normative

Rispettare i requisiti normativi più recenti, come PCI DSS, HIPAA, Sarbanes-Oxley e FISMA nel mondo fisico non è facile, ma assicurare la conformità nello spazio digitale lo è ancor meno. Negli ambienti virtuali, infatti, mancano i controlli tradizionali che sorvegliano ogni applicazione; di conseguenza è pressoché impossibile sapere quali dati sono stati utilizzati, da chi e quando e, probabilmente, questa mancanza di trasparenza metterà in allarme i revisori. Forcepoint SMC offre il livello di monitoraggio, analisi e reportistica necessario per facilitare la conformità nelle reti fisiche e virtuali. Raccoglie dati completi su tutti gli eventi di rete e li presenta in log di controllo chiari e di facile leggibilità. SMC elenca, inoltre, le impostazioni di sicurezza e segnala le modifiche apportate al sistema, offrendo report di controllo accurati e completi alla semplice pressione di un pulsante.

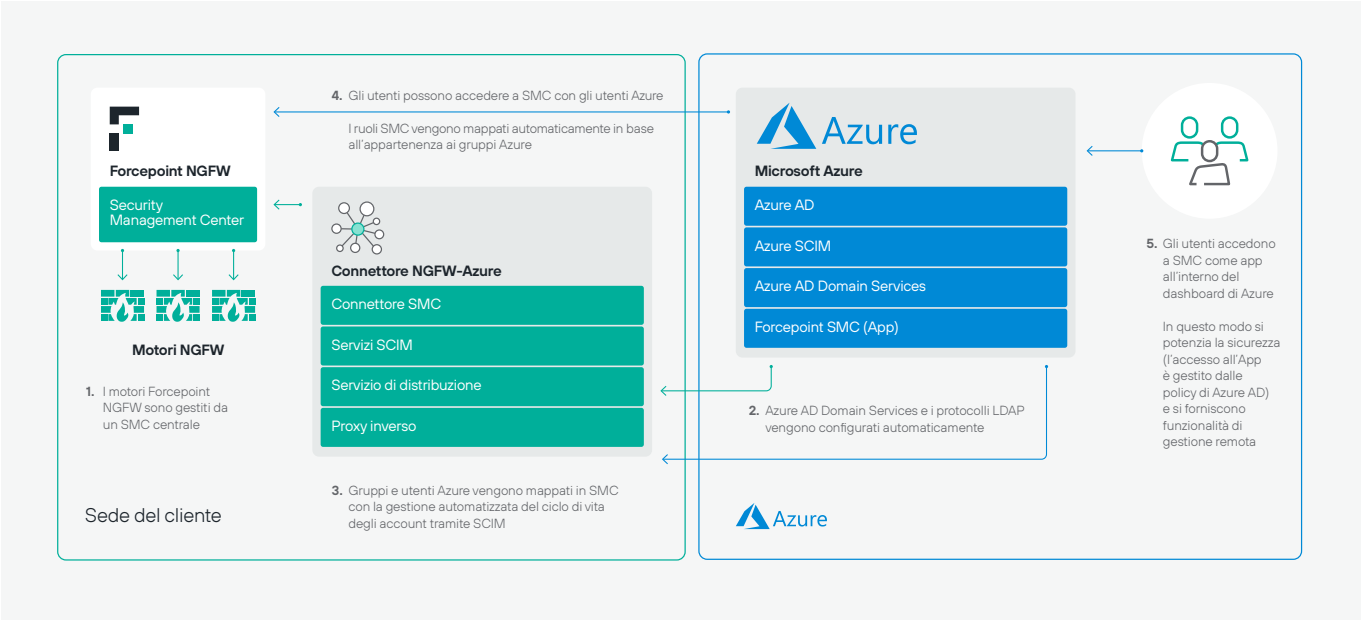
Distribuzione veloce ed elastica

Per distribuire facilmente Forcepoint Next Generation Firewall nel tuo ambiente Microsoft Azure, visita Microsoft Azure Marketplace.

→ Visita il Marketplace

Soluzioni Forcepoint Next Generation Firewall + Microsoft Azure

Ottimizza il tuo investimento in Azure e amplia le funzionalità delle tue soluzioni Forcepoint con le nostre integrazioni esclusive. Per maggiori dettagli sulle nostre integrazioni, incluse le istruzioni passo-passo per l'implementazione, visita forcepoint.github.io



Integrazione dell'accesso ibrido sicuro con Azure Active Directory (AD)

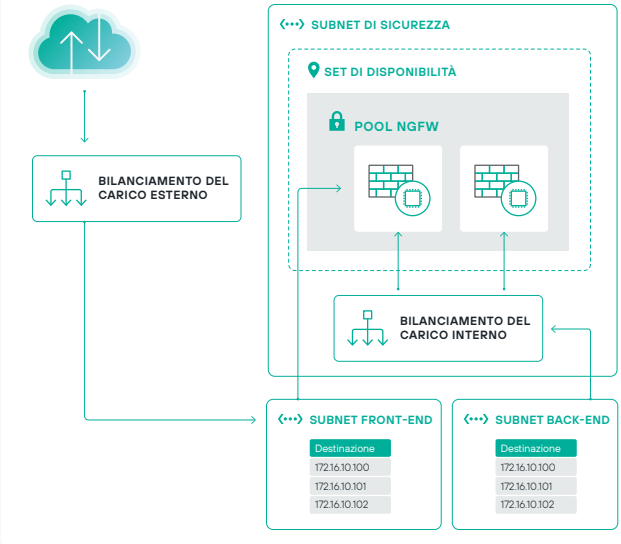
Abilita l'autenticazione e l'accesso a Forcepoint SMC tramite policy e utenti Azure AD.

- → Espone SMC come un'app Azure per offrire funzionalità di controllo remoto
- → A utenti Azure AD selezionati possono essere assegnati diversi livelli di accesso in SMC; ciò rende possibili vari scenari di gestione remota attraverso un'intera flotta di motori Next Generation Firewall
- → Abilita il controllo e la gestione centralizzati in SMC, ma con la sicurezza aggiunta delle policy di autenticazione di Azure AD

Disponibilità elevata con l'integrazione di Azure Resource Manager (ARM)

Automatizza la distribuzione di una serie ridondante di motori Next Generation Firewall in Azure, sfruttando un modello ARM configurato per distribuire l'intero stack.

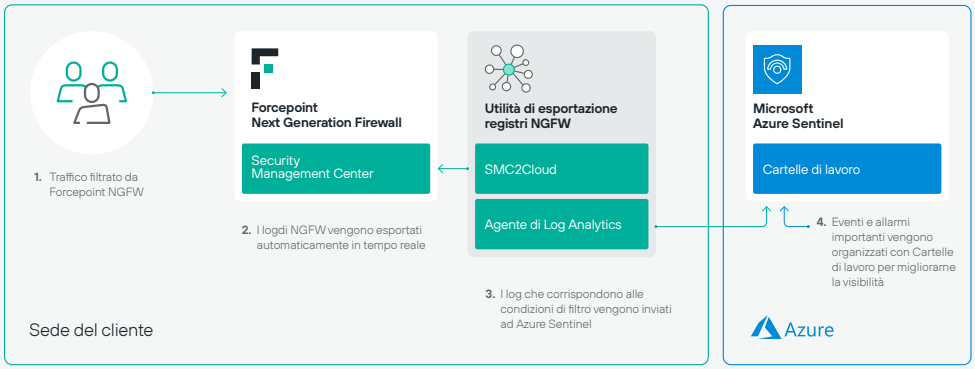
- → Modello ARM configurato per distribuire uno stack che contiene 2 servizi di bilanciamento del carico di rete e 3 subnet per gestire il traffico tra reti esterne e interne
- → Permette ai motori Next Generation Firewall di funzionare in modalità di disponibilità elevata, per assicurare un flusso di rete ininterrotto tra utenti e carichi di lavoro



Integrazione di Azure Sentinel

Consente di esportare i dati dei log pertinenti dal Next Generation Firewall, in base a filtri configurati dall'utente.

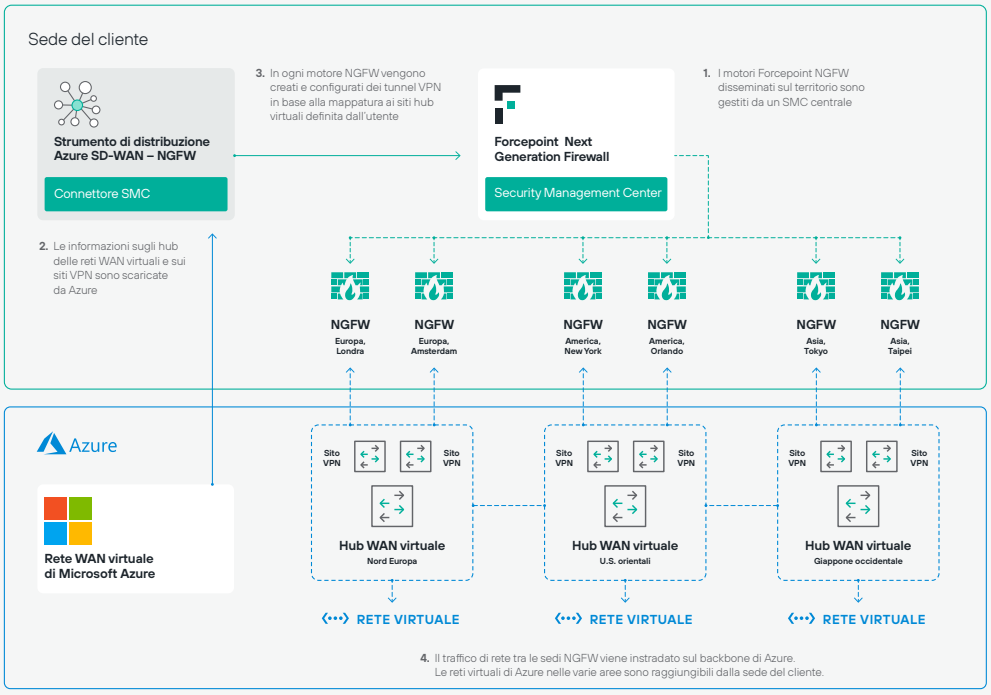
→ Esporta automaticamente gli eventi dei log da Next Generation Firewall ad Azure Sentinel in tempo reale
→ Integra i log nelle analisi dei log di Azure Sentinel e rappresenta gli eventi in formato grafico utilizzando Cartelle di lavoro



Integrazione della rete WAN virtuale di Azure

Abilita la creazione e la configurazione automatiche di tunnel IPsec tra una flotta di motori Next Generation Firewall controllati da Forcepoint SMC e siti WAN virtuali geografici.

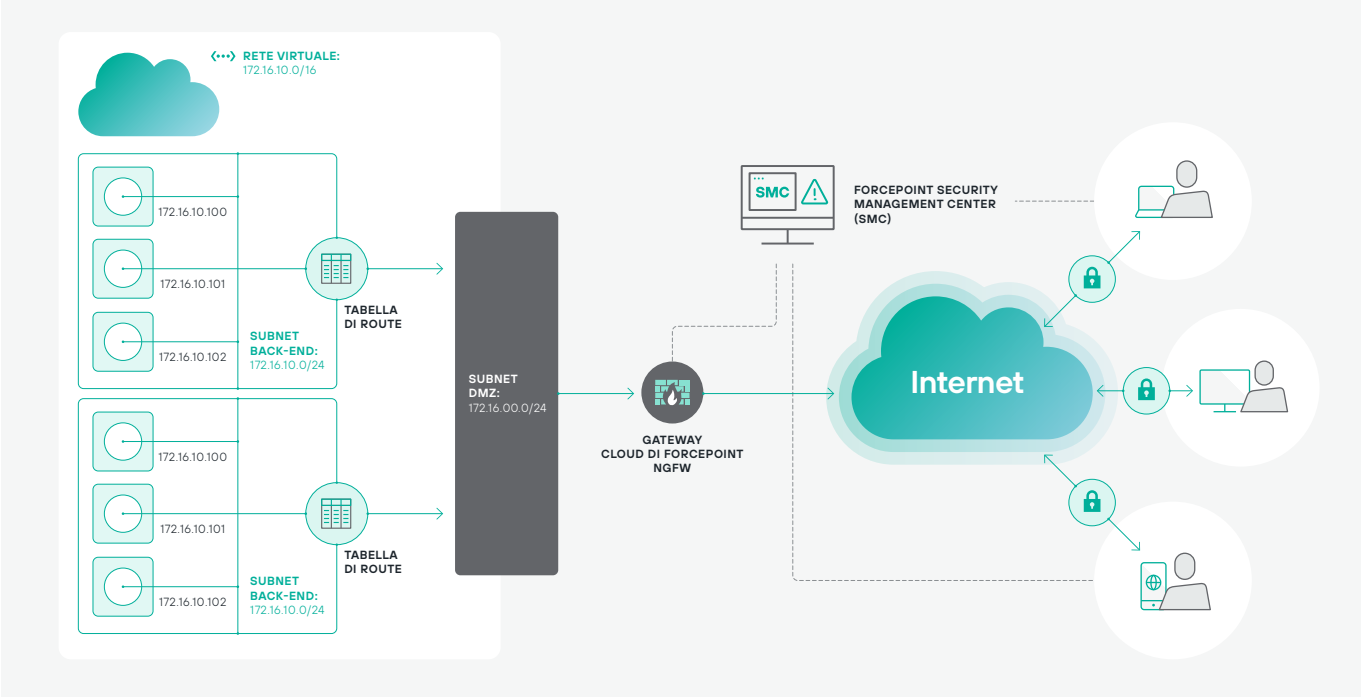
→ Crea un livello SD-WAN utilizzabile per instradare il traffico tra le sedi sul backbone della rete WAN virtuale di Azure
→ Permette agli amministratori di creare dei tunnel VPN ridondanti in ogni motore Next Generation Firewall controllato da SMC con lo standard IPsec
→ Consente di connettere dei tunnel VPN in ogni motore Next Generation Firewall a specifiche aree con la rete WAN virtuale di Azure

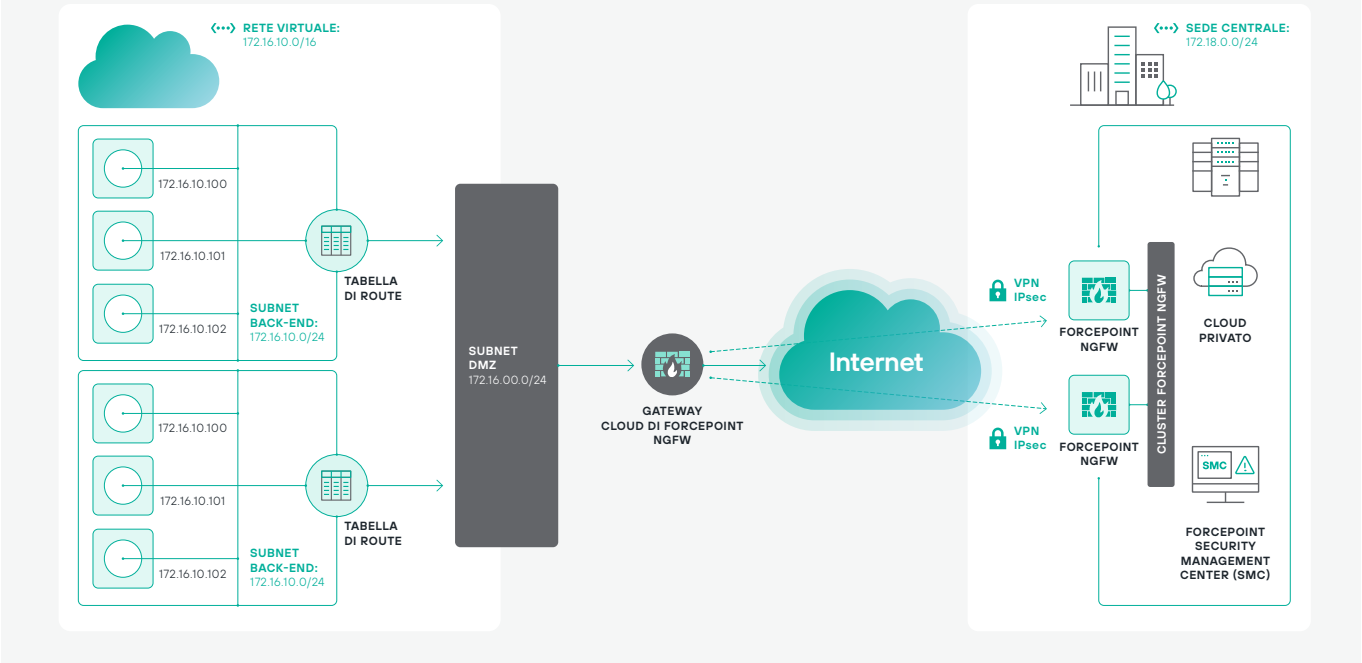


Connettività dei data center aziendali

I gateway fisici e virtuali di Forcepoint Next Generation Firewall collegano i data center aziendali locali a quelli virtuali nel cloud di Azure. Per questo caso d'uso puoi:

- → Creare semplicemente una o più connessioni VPN tra la rete del tuo data center e l'appliance VPN software di Forcepoint in esecuzione nella tua rete virtuale di Azure
- → Gestire e controllare tutti i tuoi firewall Forcepoint, sia fisici che software, a entrambi i lati delle connessioni VPN tramite SMC
- → Utilizzare anche un cluster di firewall fisici per il failover, per assicurare la continuità aziendale sul lato della connessione VPN presso la sede centrale.





Routing da VNET a VNET tra aree

Crea dei tunnel VPN sicuri tra due o più appliance VPN software Forcepoint per collegare reti virtuali all'interno o attraverso più aree Azure Cloud. Per questo caso d'uso puoi:

→ Gestire, controllare e applicare policy di sicurezza su entrambi i lati della connessione VPN utilizzando Forcepoint SMC