Integrating Hosted Security Functions with on Premises Security Functions
- Joint Force to Mitigate Internet attacks

Mohamed.Boucadair@orange.com; christian.jacquenet@orange.com ; Linda.Dunbar@huawei.com

Introduction

More and more service providers are providing hosted security solutions to deliver cost-effective managed security services to enterprise customers who face challenges with maintaining a secure infrastructure, complying with regulatory requirements, and controlling costs.

However, many medium and large enterprises have deployed various on-premises security functions which they want to continue to use. This memo advocates the combination of local security functions with remote hosted security functions to achieve more efficient counter-measures to both Internet-originated attacks and enterprise network-originated denial of service attacks. Obviously, enabling a security function does not mean that a network is protected! As such, the proposed approach can leverage on existing on-premises security functions and the expertise of service providers to properly configure those functions for a better security protection.

A typical Landscape of Enterprise Security Functions

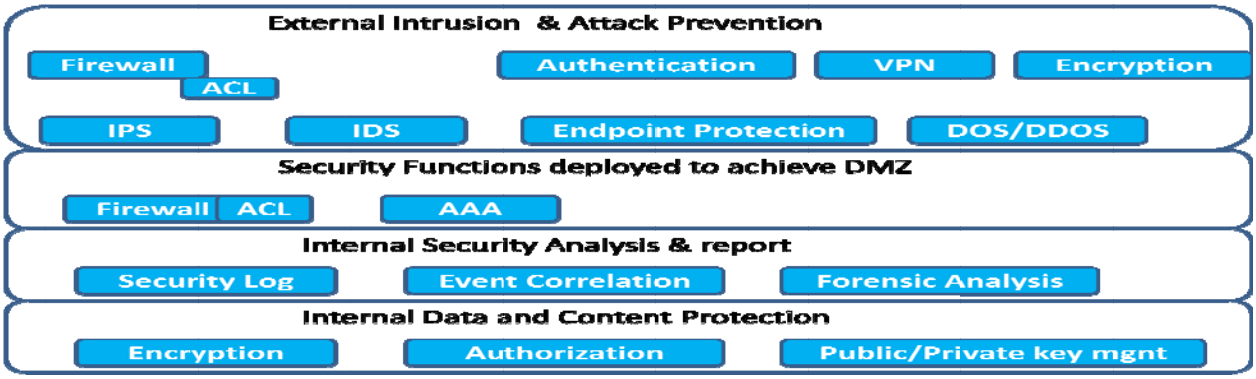

Figure 1 Various Options to Mitigate Security Threats

A value-added security service can be decomposed into elementary (sometimes virtualized) security functions that can be hosted within the same or distinct physical nodes. Any of those security functions can be potentially hosted by service providers. Some of the security strategies enforced by Enterprises rely upon the invocation of several (hosted) security functions for processing specific flows or get real time security threat feed to their on-premise security functions. Others can choose to outsource their internal security logs and Forensic Analysis to external service providers for more comprehensive threat analysis. To combine local and remotely hosted security resources for the sake of globally efficient security policy enforcement, proper mechanisms that capture enterprise security policies and to expose that information to a service provider are needed. A service provider can build distribution of elementary security functions to not only enforce the security policies desired by the enterprises but also to not alter the experienced connectivity service.

Managing Security Functions – A Provider Perspective

Service providers offering security services usually design and activate multiple security functions for their customers (e.g., outsourced firewalls, filter management, traffic encryption facilities, etc.). These service providers can provide their customers with various security functions/instances, and enforce service-specific, policy-driven, customer-driven, security-related actions accordingly. The security functions that are invoked when enforcing a security policy can be located in different equipment and sometimes be technology-specific. How a policy is translated into technology-specific actions is hidden from the customers.

For the sake of vendor-agnostic security policy enforcement, it is beneficial for security functions to have a capability index characterized by: Subject – Object – Function – Action, where:

- Subject = Match values based on information carried within the packet header or payload itself;
- Object = Match values based on contextual information associated with received packets;
- Function = Values with invoked specific security features provided by the security function; and
- Action = Values that determine how packets are handled post security features processing.

Security functions are registered to service provider based on the capability index. The enforcement of a global, customer-driven, security policy assumes the smart combination of various security functions that are either operated by customers or by the service providers. For the sake of efficiency, the combined invocation of these functions needs to be coordinated, thereby assuming reliable exchange of (security policy provisioning, log, threat feed, etc) information between the customer and the service provider. The service provider is responsible for ensuring the consistency of the global security behavior (including detect and avoid the enforcement of conflicting security policies by distinct security functions or within the same security function instance). The service provider can also detect conflicts in the requirements expressed by a customer. This is part of security service negotiation and requirements validation prior to any action on network elements.

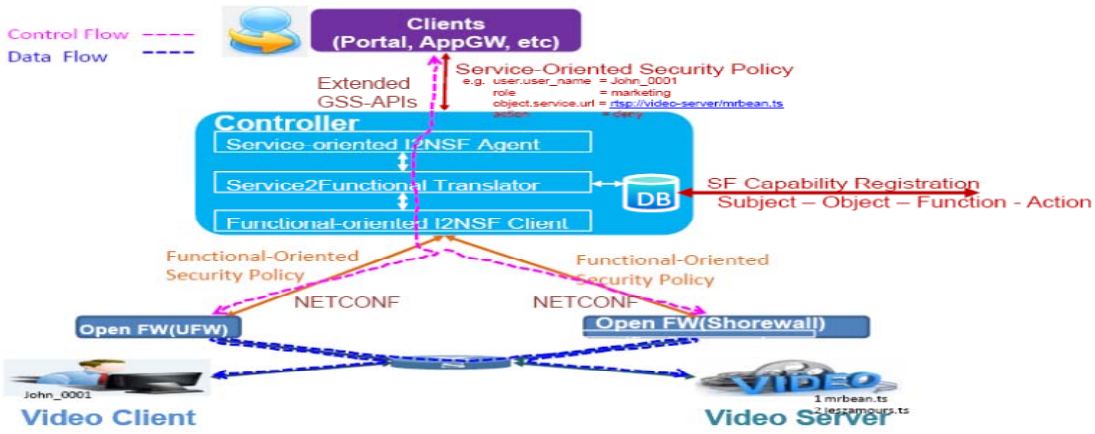

Figure 2: Security Policies from Clients to Security Functions

Interface between Customers and Security Service Providers:

Generic Security Service APIs (GSSAPI) can be used as the basis for customers to dynamically negotiate with service providers their requirements in terms of security objectives and expectations. The key feature of GSSAPI applications is the exchange of opaque messages (tokens) which hide the implementation details from the higher-level applications. Major GSSAPI routines include Credential-management routines, Context-level routines, Pre-message routines, Name manipulation routines, and other routines.

The IETF I2NSF initiative ambitions to specify additional routines for clients to express their requirements for the dynamic enforcement of flow-based security policies, based upon functions hosted by service providers, and to exchange security logs and security threat feed.

Conclusion:

To mitigate large scale security threats, the smart combination of local and hosted security functions and periodic exchange of thread feed is a promising opportunity for optimized security policy enforcement, including an improved responsiveness to massive attacks. To that aim, further standardization actions are required to unify how thread feeds are exchanged, how service requirements are captured from customers (security requirement profile), how these requirements are dynamically negotiated with service providers. Means to report attacks, actions on live network devices, or any expected degradation of the service should also be considered.