Case Study

Zero Trust Security With Next-Gen Firewall & EPP

Based on an ever-evolving unified security strategy, AhnLab provides "Zero Trust" security by integrating its Endpoint Protection Platform (EPP) with next-generation firewalls. In particular, AhnLab XTG, a new next-generation firewall launched in the first half of 2025, delivers significantly enhanced performance compared to the existing AhnLab TrusGuard and provides functionality designed for next-generation security, including Zero Trust Network Access (ZTNA).

This case study explores how endpoint-network integrated Zero Trust security is implemented by integrating AhnLab EPP with AhnLab XTG.

AhnLab EPP: At the Core of AhnLab's Unified Security Strategy

AhnLab EPP goes beyond simple security management centered on traditional point security solutions and provides stronger and more efficient threat response capabilities through cohesive endpoint security management and operations. By managing multiple endpoint security solutions through a single agent and a single management console, it enables efficient protection of complex and diverse endpoint environments.

AhnLab EPP consists of six endpoint security solutions, including the well-known antivirus solution AhnLab V3, as well as EPP Privacy Management (EPrM), EPP Patch Management (EPM), EPP Security Assessment (ESA), EPP Device Control (EDC), and EDR. Each solution provides essential security features such as virus protection, personal data protection, patch management, vulnerability assessment and remediation, device control, and threat detection and response. These capabilities are managed through a single agent and a single management console, enhancing both security and operational efficiency from the customer's perspective.

Figure 1. AhnLab EPP Configuration Diagram

Through AhnLab EPP, rules and response actions across multiple endpoint security solutions can be seamlessly linked and configured, enabling a much stronger response to security threats. Depending on the needs of security administrators, a wide range of security policies can be applied, allowing for customer-driven and proactive security operations.

AhnLab XTG: The New Next-Gen Network Firewall for Zero Trust

In the first half of 2025, AhnLab launched a new next-generation firewall, AhnLab XTG. AhnLab XTG is an advanced solution that delivers strong performance while supporting modern network security use cases such as ZTNA and SD-WAN. Its user interface (UI) is designed to be customer-friendly, providing excellent usability.

In addition, it provides features such as an intrusion prevention system (IPS), application control, VPN, C&C detection and blocking, antivirus, anti-spam, and data loss prevention (DLP). With a diverse product lineup ranging from low-end models to data center-class models, companies can efficiently deploy the solution according to their network environments.

Below is a summary of the key features of AhnLab XTG that are relevant to the operational use cases introduced in this document.

1. Application Control

AhnLab XTG is equipped with an application control feature, a next-generation security technology that enables real-time analysis and blocking, allowing, or controlling the behavior of thousands of applications, such as P2P, cloud storage services, messengers, and SNS platforms. In addition, by identifying unknown applications, it strengthens security by allowing communication only for approved applications.

2. User & Device-Based Control

AhnLab XTG identifies users not only by IP address but also by user ID, enabling classification and behavior control for efficient internal security management and rapid response to security threats. Additionally, it recognizes device status information and can control network access based on factors such as OS version, security patch status, installation of required software, and vulnerability assessment results.

3. ZTNA

AhnLab XTG's ZTNA ensures secure network access based on the core zero trust principles of "continuous verification" and "least-privilege access." It continuously verifies the identity and security posture of users and devices, allowing only verified users to access applications and network resources. By applying subdivided, application-level security policies, it enables safer remote access.

EPP & XTG Integration Case 1: Device Control Using SSL VPN

The core of device-based control integration is that the EPP server manages internal network PCs on which agents are installed, while XTG collects various types of information about those PCs from the EPP server and applies diverse firewall features, such as allowing or blocking traffic according to administrator-defined device control policies. In this process, XTG does not require a separate agent to be installed (agentless), allowing users to operate endpoint-network integrated security more efficiently.

Device-based control operation cases for EPP and XTG can be broadly categorized into ▲control based on OS version and ▲control based on V3 installation status.

1. Control Based on OS Version

Let's assume that there are still endpoints in a company running Windows 7. Windows 7 is a version for which Microsoft has ended support, making it difficult to apply patches when security issues arise. Although most systems have now migrated to Windows 10 or 11, there are cases where Windows 7 continues to be used due to unavoidable circumstances or simply because it has not been noticed.

First, when EPP identifies endpoints running Windows 7, integration with XTG allows internal network access to be permitted for those PCs while blocking Internet access and applying anti-spam functionality. In addition, access to malicious websites and C&C connections can be blocked for PCs running versions earlier than Windows 10. If there are PCs running Windows 8 or 8.1, it is also possible to apply SSL Proxy and DLP features.

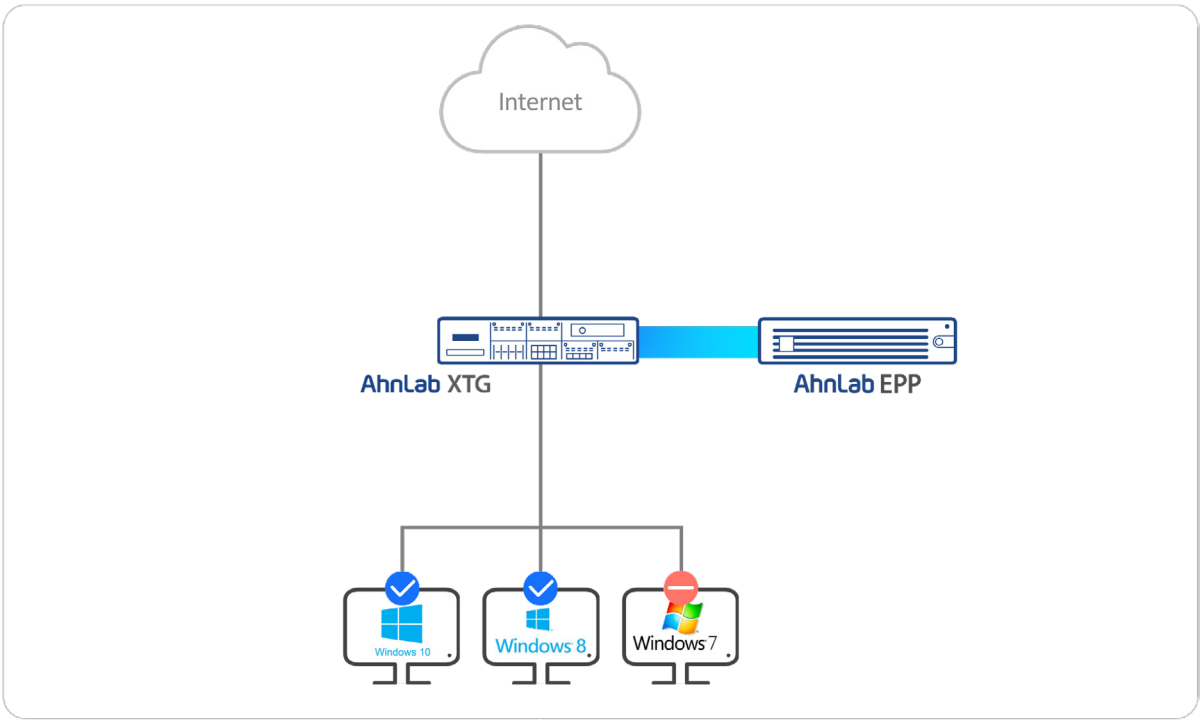

Figure 2. Control Based on OS Version

Beyond this, PCs running Windows 7 can be configured to allow only the messaging function of KakaoTalk while blocking file uploads and downloads. For PCs running versions earlier than Windows 10, remote access can be prevented, and for Windows 8 PCs, bandwidth can be limited to 1 Mbps and the number of sessions to 10,000. In this way, OS-related security information identified at the endpoint can be integrated with XTG's application and device control features to achieve highly effective security outcomes.

2. Control Based on V3 Installation Status

Controlling endpoints based on whether V3 is installed can be considered the most fundamental operation case in this scenario. If the number of employee PCs managed by security administrators is small, manual management is feasible. However, when the scale reaches the thousands or even tens of thousands, PCs without a basic anti-malware program are common.

EPP can enforce the installation of V3 through policy application. However, when such policies are not applied, PCs without anti-malware software may exist for various reasons. In such cases, the installation status of V3 can be identified, and for endpoints where it is not installed, network access can be blocked or partially allowed through integration with XTG.

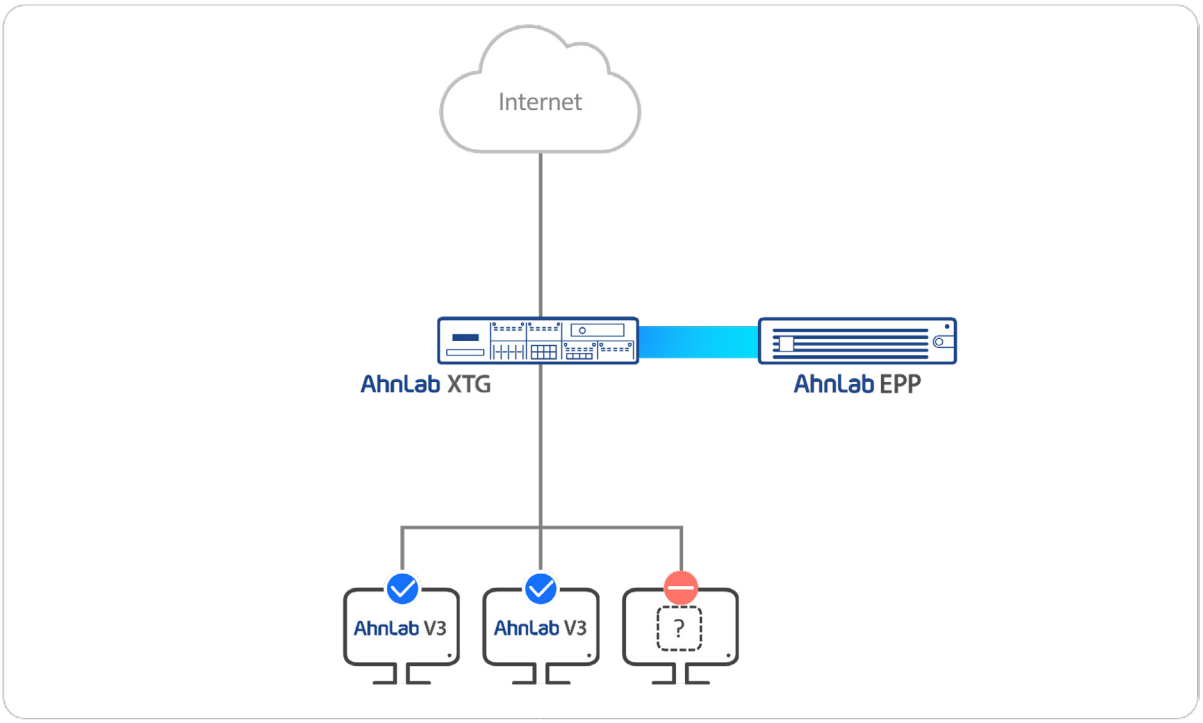

Figure 3. Control Based on V3 Installation Status

The detailed application methods are similar to the two cases described above. Access to specific external websites can be allowed only for PCs with V3 installed. For messaging services, access can be blocked for PCs without V3, while allowing KakaoTalk file uploads and downloads only on PCs where V3 is installed. In addition, PCs without V3 installed can have all security threat response features applied, such as intrusion prevention systems (IPS), web filtering, anti-spam, and malicious site blocking. In this way, a wide range of security policies can be applied depending on the presence of V3.

EPP & XTG Integration Case 2: EPP Agent Redirection

The EPP agent redirection feature ensures security by guiding PCs without an EPP agent installed to install the agent when they attempt to communicate over the Internet. In terms of operation, when a PC without an EPP agent attempts Internet communication, XTG redirects the traffic to the EPP server, which then presents a page prompting agent installation. Subsequently, only PCs with the EPP agent installed are allowed to use the network.

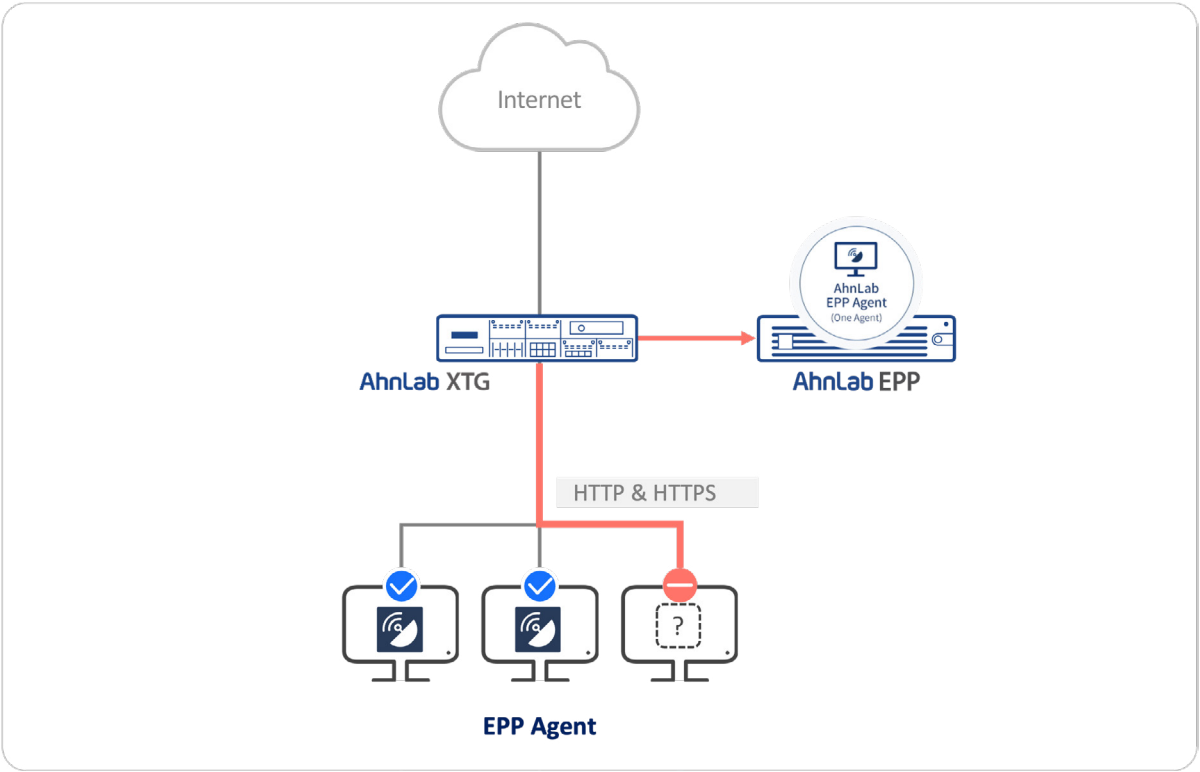

Figure 4. EPP Agent Redirection

From the user's perspective, this feature is effective when planning a new EPP deployment or when EPP is already in use and agent redirection is desired for HTTPS web access. This is because XTG provides this feature for both HTTP and HTTPS traffic. Additionally, if the network is in a network address translation (NAT) environment and EPP agent redirection is not possible, the issue can be resolved by using XTG as the NAT device.

EPP & XTG Integration Case 3: ZTNA – ESA Integration

Recently, the number of organizational connection points has been increasing, such as branch office–headquarters, partner company–headquarters, and remote work. It has become necessary for organizations to establish security systems that support these diverse connection scenarios, and this is an area that many enterprises are actively considering.

AhnLab XTG applies ZTNA to enable secure access to internal networks. However, even when ZTNA is used, issues can arise if an external endpoint is infected with malware or has been compromised by a hacker. Therefore, it is critically important to verify the security status of the remote endpoints themselves before allowing access to internal systems.

AhnLab integrates ESA, a component of EPP, with XTG's ZTNA to allow remote access only from secure endpoints. In simple terms, the XTG ZTNA Client checks the endpoint's security assessment score and allows ZTNA login only when the score meets the threshold configured by the administrator. For example, a policy can be applied that permits access only when the security assessment score exceeds 90 points. In addition, the ESA assessment score is evaluated on a per-minute basis, ensuring real-time enforcement.

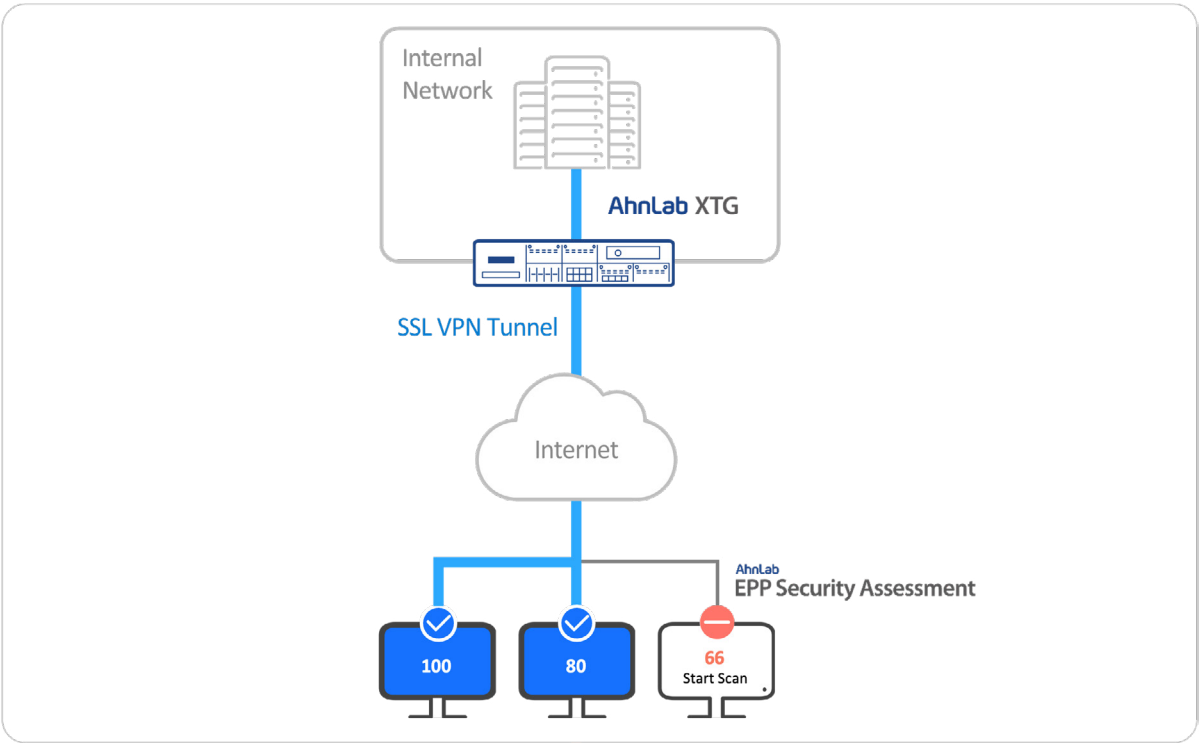

Figure 5. ZTNA – ESA Integration

From the customer's perspective, this enables the creation of a stable business environment by combining "secure endpoints" with "zero-trust access." This approach is effective in situations where it is impossible to apply and manage security on endpoints used by remote workers or external partners accessing the internal network, or in various other remote access scenarios where organizations wish to permit internal network access only after verifying a minimum level of endpoint security.

Conclusion

The recent security landscape can be summarized by two key trends: ▲increasingly sophisticated threats ▲growing security complexity. In other words, as attack techniques become more advanced, organizations face greater security complexity, requiring them to deploy many solutions and analyze an increasing volume of security data.

An effective strategy to address these two challenges is unified security. As demonstrated by the endpoint-network integrated security operation cases discussed here, when organizations apply a unified security strategy correctly, they can build a stronger and more efficient zero trust security framework and establish a stable business environment.

We hope that organizations considering a Zero Trust strategy will adopt a unified security framework and enhance their long-term business competitiveness.

AhnLab

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com/en | global.sales@ahnlab.com