SOLUTION BRIEF

ZTNA Over VPN Tunnels

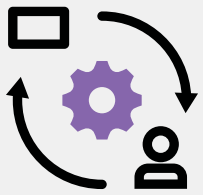
How Fortinet Can Help Apply ZTNA Principles to a VPN Infrastructure

Executive Summary

Zero-trust network access (ZTNA) is a key component of the zero-trust security model, which advocates for "never trust, always verify" principles. ZTNA reduces the attack surface of organizations by verifying users and devices before granting them access to applications. Then, it continuously monitors the users and devices for changes in security posture.

ZTNA is gaining popularity as a starting point for many organizations on their zero-trust journey. It is a foundational element of the zero-trust executive order issued by the U.S. government in May 2021, which requires federal agencies to implement zero-trust security principles by 2025. By focusing on who and what has access to applications, ZTNA is a big step forward in reducing organizations' attack surfaces.

For all the benefits of ZTNA and talk about how it will replace virtual private network (VPN) tunnels, many organizations are still interested in utilizing their VPN infrastructure and applying ZTNA principles to application access. This solution brief shows how to do this using Fortinet equipment. This use case is best described as ZTNA over VPN.



Evaluating ZTNA Solutions
When evaluating ZTNA solutions, it is a good practice to confirm that the vendors being considered do enforce these principles. A proof-of-concept (POC) test is a good tool to verify actual performance.

Access Only for Correct Users and Devices

At its core, ZTNA is about controlling access to applications with an "always verify" approach. ZTNA verifies user and device identity, often using multi-factor authentication (MFA) and certificates to ensure that only the correct ones have access.

ZTNA checks the contextual information about the user, such as their role, location, time of day, and device type, to ensure that it matches the policy for accessing an application. It also validates the device's posture to ensure that only appropriately configured devices can access applications.

ZTNA only grants access to a specific application for a single session. Every access request is verified, regardless of the user or application. Then, by continuously checking on users and devices, ZTNA eliminates access to applications if any contextual information changes. This frequent and complete verification approach reduces an organization's attack surface, making it much harder for bad actors to gain or maintain access to an application.

Security Posture Tags

A security posture tag is a mechanism the FortiClient EMS uses to identify when an endpoint has met a certain condition, such as whether the antivirus application is turned on or if it has updated firmware. The security posture tag is provided to the FortiGate to evaluate any policies for that endpoint.

This system allows for real-time device posture checking, as the Endpoint Management Server (EMS) reports on endpoint tags every minute. Furthermore, EMS can ingest information from FortiEDR or FortiSIEM that can then be incorporated into a security posture tag.

FortiSIEM can tap information from many different sources, which magnifies the contextual information available for ZTNA policies. The FortiGate will check the security posture tag status before granting access to an application.

ZTNA Over VPN Tunnels

Using a known and trusted technology can be a good way to start adopting zero-trust principles. Leveraging existing equipment and providing minimal changes can be a safe first step on a zero-trust journey. ZTNA over VPN tunnels will provide many of the core principles of a full ZTNA solution, but will not provide:

- Automatic, encrypted tunnels from endpoint to application
- Encrypted communications when on the internal network
- Granular access to a single application session, as the VPN tunnel alone, typically provides networkwide access

In FortiGate Next-Generation Firewalls (NGFWs), these capabilities do come with a full, proxy-based ZTNA solution using a ZTNA application gateway. That said, many of the benefits of a full ZTNA solution can be realized with ZTNA over VPN tunnels. Among those benefits are:

- Using encrypted tunnels for remote access to applications over the internet
- Using FortiGate NGFW policies to set up many of the checks of a full ZTNA solution, including:
  - Creating user identity policies to restrict access to each protected application
  - Configuring access policies to check for user contextual information such as time of day and geolocation
  - Checking the identity of the device via the EMS device certificate
  - Checking EMS security posture tags to verify the device's posture
  - Using the security posture tags to identify what conditions the device might or might not have

  Note: Contextual checks continuously use security posture tags.

Additionally, ZTNA over VPN tunnels has the following benefits:

- Supporting all types of traffic, including web, TCP, and UDP
- Using existing infrastructure, such as VPN endpoint agents and concentrators, for a secure and well-understood architecture by users and administrators
- Saving training costs, procurement costs, and speeds adoption of zero-trust concepts

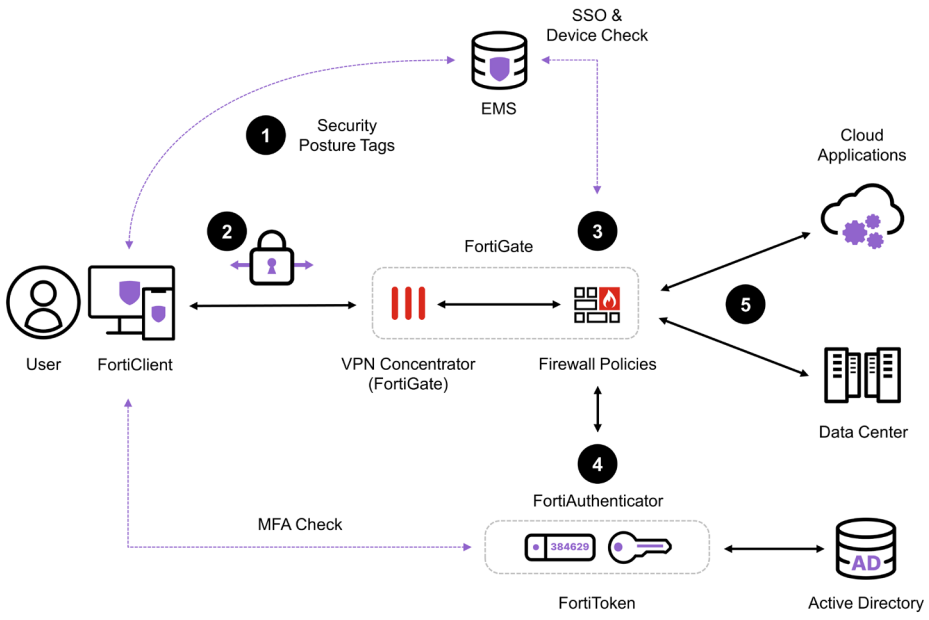


Figure 1: ZTNA over VPN tunnels architecture

ZTNA Over VPN Tunnels vs. Full VPN Comparison Chart

	ZTNA over VPN	Full ZTNA
User identity authentication	**Yes**	**Yes**
Device identity	**Yes**	**Yes**
Device identity authentication	**No**	**Yes**
Device posture	**Yes**	**Yes**
Granular application access	**Yes**	**Yes**
Application segmentation	**No**	**Yes**
TCP, RDP, web support	**Yes**	**Yes**
UDP support	**Yes**	**No**
Continuous checking	**Yes**	**Yes**
User contextual information	**Yes**	**Yes**
Device contextual information	**Yes**	**Yes**
Automatic, per-session encrypted tunnel	**No**	**Yes**
Networkwide access	**Yes**	**No**
Internal encrypted communication	**No**	**Yes**
Uses FortiClient	**Yes**	**Yes**

Summary

ZTNA is a good place to start on your organization's long zero-trust journey. ZTNA over VPN tunnels is not a full ZTNA solution. However, it does significantly improve the level of zero-trust controls for controlling access to applications using a familiar infrastructure and tools. ZTNA over VPN tunnels can pave the way toward zero trust with an easier transition to a full ZTNA solution in the future.

November 2, 2023 11:08 AM
2411126-0-0-EN