SECFENSE GHOST

Ghost for Citrix /NetScaler Gateway

Make it **unreachable to the internet.** Keep it fully operational for verified users.

WHO THIS DOCUMENT IS FOR

A two-page brief for security and network teams: how to remove the public attack surface of Citrix NetScaler Gateway without replacing it.

THE EXPOSURE PROBLEM

Reachability, not severity, decides who gets exploited first.

NetScaler Gateway sits directly on the perimeter, which turned memory-safety flaws into credential-harvesting at internet scale. Both CitrixBleed generations were exploited against reachable gateways within days.

~5 days

from disclosure to exploitation, industry-wide

32 days

median time organizations take to patch

For a reachable gateway, the patching race is unwinnable by design.

PUBLICLY KNOWN INCIDENTS	WHAT IT ENABLED
CVE-2023-4966 · CitrixBleed	Session token theft from memory; widely used by ransomware groups for initial access.
CVE-2025-5777 · CitrixBleed 2	Out-of-bounds read leaking session tokens; millions of attack attempts observed, financial sector hit hardest.
CVE-2025-6543 · buffer overflow	Critical (CVSS 9.2), added to CISA KEV while exposed gateways were still unpatched.

WHAT GHOST DOES

Secfense Ghost is a **pre-access layer** that makes Citrix NetScaler Gateway unreachable from the public internet by default.

A network path exists only for users who have just proven they belong to your organization — through a corporate-domain e-mail address or an organization-issued PKI certificate — and only for the duration of a time-boxed session.

To scanners, exploit kits and zero-days, **the gateway does not respond at all.**

This is not security by obscurity.

Security by obscurity relies on a secret that can leak: a hidden port, an unlisted URL, a magic knock. Ghost has no secret. It enforces **default-deny at the network edge** — no handshake, no banner, no login page, even for attackers who know the exact address.

A route opens only after the user proves membership in the organization: control of a corporate-domain mailbox or an organization-issued PKI certificate.

Invisibility is not the security mechanism — it is the result of it. This is **authenticate-before-connect** , the core zero-trust principle, applied at the network layer.

HOW IT WORKS WITH CITRIX NETSCALER GATEWAY

Verification happens before reachability.

01 **Deny by default**

The gateway drops every packet from the public internet. No handshake, no banner, no attack surface.

02 **User requests access**

An employee opens the Ghost access point; their source IP is detected automatically.

03 **Organizational verification**

The user proves organizational membership: corporate-domain e-mail or an organization-issued PKI certificate.

04 **Route opens**

The verified IP is published to the gateway allowlist, scoped to that user and session.

05 **Access expires**

The TTL lapses, the entry is removed, and the gateway goes dark again.

INTEGRATION NOTE

Ghost automates NetScaler ACLs and policy objects through the NITRO API: a verified user IP is allowed for the duration of the session TTL, then removed. Gateway virtual servers, ICA proxy and existing authentication policies continue to work exactly as before.

Deployed in about 2 hours.

Nothing gets reorganized.

Deployed in about 2 hours

Ghost sits in front of what you already run. The first gateway is typically protected within about 2 hours — not as part of a migration program.

Your infrastructure

Deployed on-prem or in your cloud. User traffic never routes through anyone else's cloud — ours included.

No network redesign

No new tunnels, no re-architected routing, no agents to mass-deploy. Topology stays as it is.

Nothing new for users

One lightweight step before connecting: corporate e-mail confirmation or a certificate already on the device. The client stays the same.

COMPLIANCE

NIS2 Art. 21

Requires risk-proportionate technical measures including access control and network security. Removing public reachability of access systems is a direct, demonstrable risk reduction.

DORA

Requires financial entities to minimize their ICT attack surface. Ghost removes public reachability and gates every route on verified organizational identity — corporate e-mail domain or PKI certificates.

WHAT GHOST IS NOT

Not a patching substitute. An unreachable gateway removes opportunistic exploitation and buys time, but vulnerable software should still be patched.

Not a full ZTNA platform. Ghost governs who can reach the gateway, not per-application micro-segmentation behind it.

Not magic for every network. CGNAT or heavily shared egress IPs require one of Ghost's alternative deployment modes; we qualify this before you commit.

See exactly what attackers see.

Request a free **Exposure Report** : a passive scan of your public perimeter, reviewed by a Secfense engineer, delivered within 24 hours. No installation, no access to your systems required.

Request your Exposure Report →

Contact Sales


SECFENSE