

LinTrust CyberWallOS 3.0 Announcement

Frequently Asked Questions

Q: 什么是 CyberWallOS?

A: CyberWallOS 是领信系列防火墙产品的内核名称。CyberWallOS 负责驱动防火墙所提供的所有安全功能和所有的管理配置功能。CyberWallOS 3.0 是安氏目前发布的最新版本。

Q: CyberWallOS 3.0 可支持领信防火墙的哪些型号？

A: 目前，领信防火墙的以下型号可以支持 CyberWallOS 3.0

- LinkTrust CyberWall-100SE
- LinkTrust CyberWall-100HP
- LinkTrust CyberWall-100Pro
- LinkTrust CyberWall-100Pro-T
- LinkTrust CyberWall-204
- LinkTrust CyberWall-206F
- LinkTrust CyberWall-206SP
- LinkTrust CyberWall-1000F
- LinkTrust CyberWall-1000A

Q: CyberWallOS 3.0 新增的特性都有哪些？

A: CyberWallOS 3.0 包含了 CyberWallOS 2.8 提供的所有特性，并新增了以下内容：

1. 多端口防火墙 (Multiple Interface Support)

- 设计能力支持多达 64 个物理以太网接口
- 每个物理接口可配置多个 VLAN 逻辑子接口，VLAN 逻辑子接口与常规接口具有等同的配置能力
- 对称安全性设计，所有物理接口与 VLAN 逻辑子接口具有等同的特性与攻击防护功能，扫除来自网络各个区域的安全威胁。
- 提供带外管理功能，可自定义 MGT 管理接口，定义为 MGT 属性的接口专用于管理防火墙使用，管理流量与其他网络通讯流量分开。用户可自己选择是否定义 MGT 接口
- 可自定义 IDS 流量镜像接口，定义为 IDS 属性的接口专用于流量镜像使用。用户可自己选择是否定义 IDS 接口
- 可自定义 HA 心跳口，定义为 HA 属性的接口专用于 HA 心跳通讯使用。用户可自己选择是否定义 HA 接口

2. 安全域(Security Zones)

- 多安全域防火墙，可配置多达 32 个自定义域
- 基于安全域的策略设置
- 每个安全域中可配置多个物理接口和 VLAN 子接口
- 域内网络对象的访问控制

3. 802.1Q Vlan Trunk

- 路由模式下支持 VLAN 协议
- 透明模式下支持 VLAN 协议

4. 动态 VPN 网关

- ADSL VPN 网关支持
- DHCP VPN 网关支持

5. DHCP 中继代理

CyberWallOS 3.0 提供 DHCP 中继功能，可以在所有的物理接口和 VLAN 逻辑接口上配置中继代理功能，可支持多达 8 台 DHCP 服务器的中继

6. VPN 拨号用户的访问控制

在 CyberWallOS 3.0 中增加了对 VPN PPTP 拨号用户的访问控制功能。对于启用了 VPN 功能的防火墙，系统会默认建立 PPTP 域，并将 VPN 拨入的用户自动分配到这个 PPTP 域，拨号用户对内部资源的访问由 PPTP 域的访问控制策略决定。

7. 简化的 VPN 星型部署

CyberWallOS 3.0 支持最简化的 VPN 星型部署方式，各地分节点的防火墙只需与中心点防火墙配置 1 条 VPN 隧道即可完成各地之间、各地与中心的全网的 VPN 通讯。

Q: 我在哪儿能找到一份关于 CyberWallOS 3.0 新功能的详细技术描述？

A: 在《LinkTrust CyberWallOS 3.0 发布说明》中完整的讲述了 3.0 的新增特性，另外在《领信防火墙技术白皮书 v.30》中也含盖了这些内容。以上资料可以从 http://bj.is-one.net/LinkTrust_Cyberwall/support/document.dhtml 下载。

Q: 作为 LinkTrust CyberWall-100 型号的用户，我为什么要升级 CyberWallOS 3.0 版本？

A: CyberWallOS 3.0 采用全新的灵巧安全网关架构 FSGA(Flexible Security Gateway Architecture)，设计能力支持多达 64 个物理以太网口和上千个 VLAN 逻辑子接口，提供完全对称的配置及防护能力，结合灵活的安全域定制，策略设置更加随心所欲，可轻松适应甚至是最复杂的网络环境。另外，FSGA 的引入使得一系列安全功能成为可能，这里面已经有很多在 OS 3.0 中得以实现，FSGA 架构将成为 CyberWallOS 的发展基石，并且将支持领信防火墙家族推出的所有产品。CyberWallOS 3.0 是领信防火墙发展的里程碑。

Q: 什么是 FSGA？它与 CyberWallOS 3.0 有什么联系？

A: FSGA (Flexible Security Gateway Architecture)是安氏安全实验室最新为 CyberWall 设计的体系结构，它旨在解决传统防火墙所存在的种种局限以及提供更适应现代企业安全

需求的强大功能。CyberWallOS 3.0是采用 FSGA 架构的第一个版本。关于 FSGA 更详细的技术介绍，请参见《领信防火墙技术白皮书 v3.0》，您可以从 http://bj.is-one.net/LinkTrust_Cyberwall/support/document.dhtml 下载获得。

Q: 如果从低版本升级到 CyberWallOS 3.0，我原先的策略配置能兼容吗？

A: CyberWallOS 3.0的设计充分考虑了策略兼容性问题，保证了系统的平滑升级。用户不必担心升级 3.0 后需要重新配置策略，或是担心网口顺序发生改变。系统会自动将旧策略调整到支持 OS3.0 的策略格式，调整过程完全由系统完成。

Q: 为什么在升级完 CyberWallOS 3.0 后，用 Web 管理防火墙时会出现“发现加载脚本出现错误”的提示窗口？

A: 前面已经提到，升级 3.0 后，系统会自动将旧策略调整到支持 OS3.0 的策略格式。但先前版本中有一些内含的系统指令对新版本已经不再适用，Web 窗口中显示的就是这些指令。用户完全不必关心这些内容，因为这些系统内含指令已完全被新版本所替代，不会对用户的正常使用产生影响。用户手工保存(save)一下防火墙的配置，下次管理防火墙时就不会再次出现这样的提示信息了。

Q: 升级 CyberWallOS 3.0 后，如果我想 Restore 原来的旧版本使用可以吗？

A: CyberWallOS 3.0 目前不支持策略的倒退兼容。系统无法将 OS 3.0 的策略格式自动调整回低版本支持的格式。所以，如果用户想退回原来的旧版本使用，则需要手工调整策略或使用原来备份的策略文件。建议用户在升级 OS 3.0 前，先备份原先的策略配置。

Q: 升级 CyberWallOS 3.0 后，还需要重新申请 License 吗？

A: 如果产品已经安装有 License，升级 CyberWallOS 3.0 后，不需要重新申请新的 License。
注：用户在升级前务必保证防火墙已经安装了 License(许可证)。可在命令行管理模式下输入"#show License" 以确定是否安装过许可证，如果尚未安装请与安氏客户服务中心联系，只有在安装许可证后才能进行升级。

Q: 我原来购买的是带 IDS 镜像口的 4 网口防火墙，通过 CyberWallOS 3.0 的升级，能使它升级成真正的 4 网口防火墙吗？

A: 是的，完全可以，这正是 CyberWallOS 3.0 的优势之一。在 CyberWallOS 3.0 发布之前，第 4 个网口专用于 IDS 流量镜像，不用于网络通讯。在升级完 CyberWallOS 3.0 之后，第 4 个口与常规端口具有等同的特性与配置能力，完全可以作为真正的 4 口防火墙使用。

Q: 我原来购买的是带 IDS 镜像口的 4 网口防火墙，如果升级了 CyberWallOS 3.0，还具有 IDS 镜像功能吗？

A: 在升级完 CyberWallOS 3.0 之后，第 4 个口默认作为通讯网口使用，用户可以象使用

其他网口一样，在这个网口上挂接通讯网段。 如果用户想继续将此网口作为 IDS 镜像口使用，可以在命令行管理模式中使用 Fix Function 功能将此网口配置成 IDS 口

Q: 作为领信防火墙的用户，我从哪儿可以获得 CyberWallOS 3.0 ?

A: OS 3.0 可以从 http://bj.is-one.net/LinkTrust_Cyberwall/support/download.dhtml 下载。每种型号产品的升级对应各自的内核升级文件，用户在升级前可根据产品的序列号或通过当地经销商确认产品型号，下载相应型号的内核文件进行升级。