endian

Secure everyThing

Endian Security Administrator Training

Module :: SSL VPN (OpenVPN)

ESAT endian

endian
Secure everyThing

Module
VPN

SSL VPN Introduction

The Endian UTM appliance provides a complete SSL VPN solution built using the popular **OpenVPN** application. Endian can provide (1) Net2Net connections for building tunnels between devices which can be useful for connecting two or more offices together and (2) remote access (roadwarrior) connections for end-users to connect using their computer in order to access internal network resources.

endian
Secure everyThing

Module
VPN

SSL VPN Advantages

- **Universal Platforms:** Endian has a native client for every major platform including Microsoft Windows, Mac OS X, and Linux (Redhat / Ubuntu)
- **It Just Works:** Because it runs in user-space it's more versatile and can support tunnels from dynamic IP addresses, works perfectly behind NAT, and can even be tunneled from the client-side over TCP 80/443 to work behind existing firewalls
- **Proven Security:** Built using SSL/TLS technology which is considered to be one of the strongest and most mature protocols (e.g. HTTPS); in addition, Endian by default uses two-factor security that requires both a certificate and a valid username/password combination
- **Scalable, Stable & Efficient**: This means you can support lots of tunnels without consuming much resources and the product is rock-solid

endian
Secure everyThing

Module
VPN

SSL VPN Advantages

- **Completely Flexible:** Use either TCP or UDP to suit your requirements and you only require a single port on the server-side to be open on a public IP address
- **Routed or Bridged:** Use either bridged mode (default) to provide a virtual Ethernet connection like your were physically plugged-in or use routed mode to provide a completely separate and dedicated VPN network
- **Client Customization:** Control the parameters pushed out to each VPN client like custom route(s), DNS server addresses, and domain suffix
- **Intra-Client Traffic:** Control whether clients are allowed to see and communicate with each other while connected to the VPN server
- **Dedicated Client:** Endian Connect App allows seamless connection to Connect Switchboard and any OpenVPN Server
- **3rd Party Clients:** Open and extensible OpenVPN server supports virtually any OpenVPN client on any platform.

endian
Secure everyThing

Module
VPN

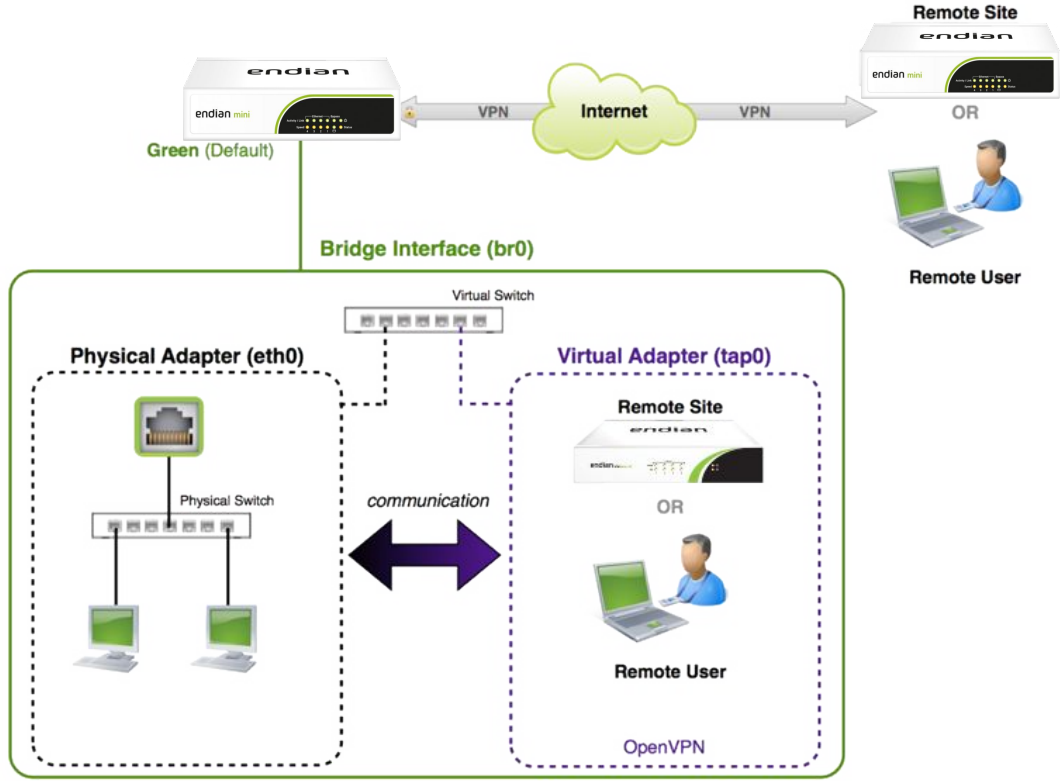
SSL VPN Advantages

- **External User Authentication:** Support for syncing SSL VPN groups and users to an external Active Directory or LDAP server
- **Multiple Server Instances*:** Create multiple (unique) OpenVPN server instances to increase the performance and scalability of your server as well as provide fail-back support (try UDP then fail to TCP)
- **Multi-Core Balancing*:** Assign each instance a set number of CPU cores to allow for the scaling of each instance with the right amount of resources
- **TUN Mode Support:** Now supports TUN mode (in addition to TAP) which allows connections from the OpenVPN Client Connect mobile app (iOS/Android)

endian
Secure everyThing

Module
VPN

SSL VPN Architecture



endian
Secure everyThing

Module
VPN

SSL VPN Architecture

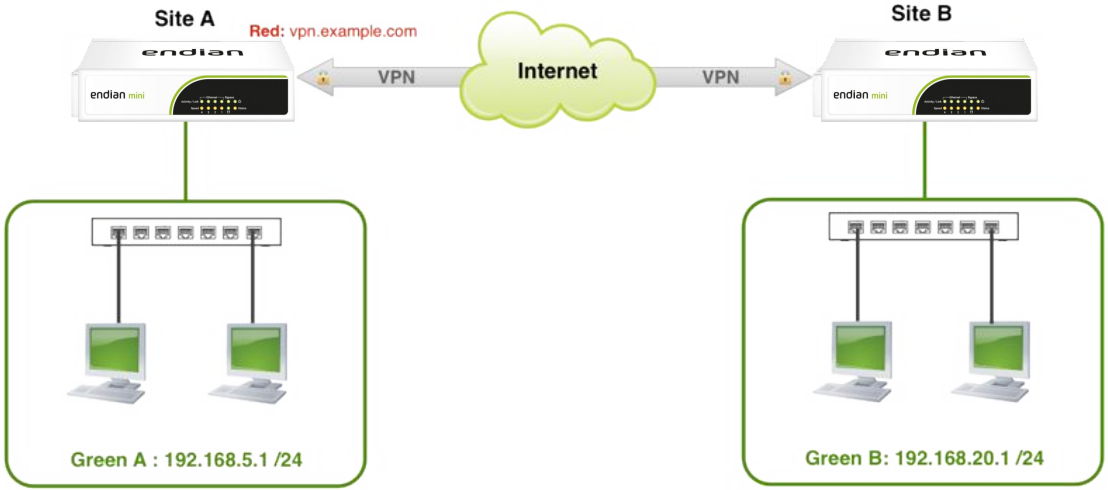
- **Virtual Ethernet:** For remote access (roadwarrior) connections, the SSL VPN connection from a client machine will get an IP inside the Green network bridge which means it will be analogous to being plugged in physically (and even pass broadcast traffic).
- **Bridge to Any Network:** You can bridge the SSL VPN server to any internal network zone (Green, Blue, Orange) and get a virtual Ethernet connection.
- **Push Client Settings:** With the Endian SSL VPN client you can push information (at any time) to the client including things like DNS servers, domain suffix, additional network routes, and more.

DHCP Note: *Even though the Endian SSL VPN server uses IP addresses inside the Green subnet -- it has its own internal DHCP server that is separate from the Endian network DHCP (Services > DHCP).*

endian
Secure everyThing

Module
VPN

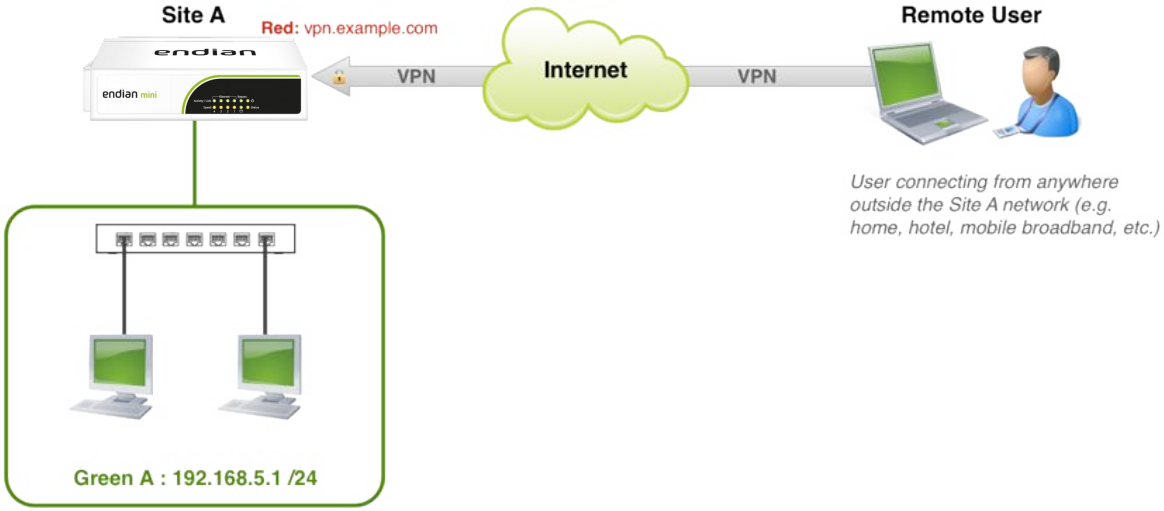
SSL VPN Net2Net



endian
Secure everyThing

Module
VPN

SSL VPN Remote Access



endian
Secure everyThing

Module
VPN

2-Factor VPN Authentication

Two-factor authentication provides a second layer of security to any type of login, requiring extra information or a physical device to log in, in addition to your password. For Endian, this means having both:

Something you know (a unique username and password)

Something you have (a time-based token on your smartphone)

endian
Secure everyThing

Module
VPN

Why 2-Factor Authentication

Two-factor authentication is one of the best ways to protect against remote attacks such as phishing, credential exploitation and other attempts to takeover your accounts. Without your physical device, remote attackers can't pretend to be you in order to gain unauthorized access to corporate networks, cloud storage, financial information, etc.

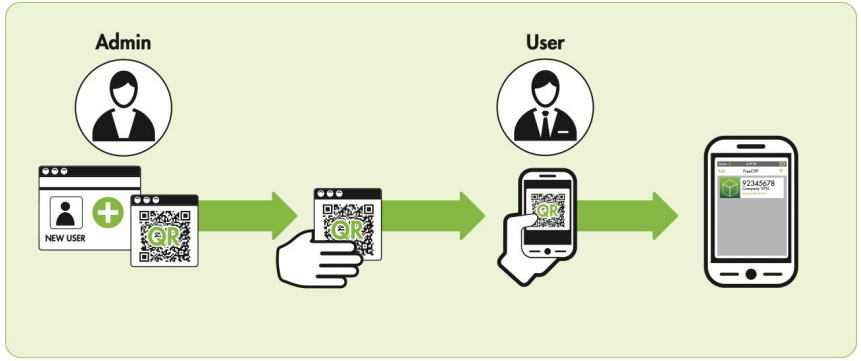
Verizon's Data Breach Investigations Report (DBIR) found that 95 percent of breaches involve the exploitation of stolen credentials. Many recent high-profile breaches can be traced back to stolen passwords, either from third-party vendors or from corporate employees.

endian
Secure everyThing

Module
VPN

2-Factor VPN Authentication

Process Diagram



endian
Secure everyThing

Module
VPN

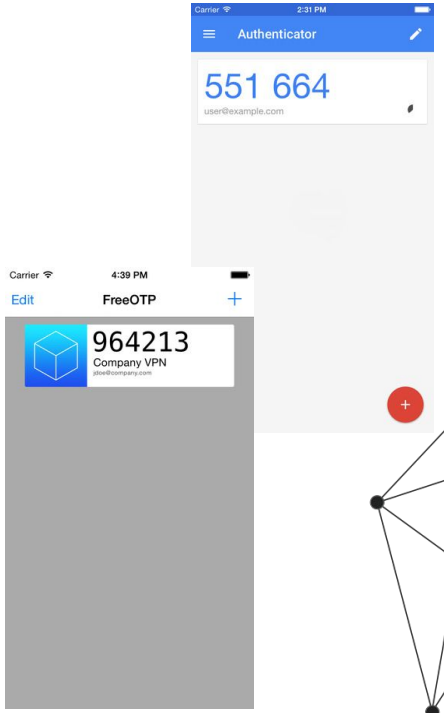
2-Factor VPN Authentication

Supported (Free) OTP Mobile Applications

iOS
Google Authenticator, FreeOTP

Android
Google Authenticator, FreeOTP

Windows Mobile
Microsoft Authenticator



endian
Secure everyThing

Module
VPN

2-Factor VPN Authentication

Using Endian Connect App

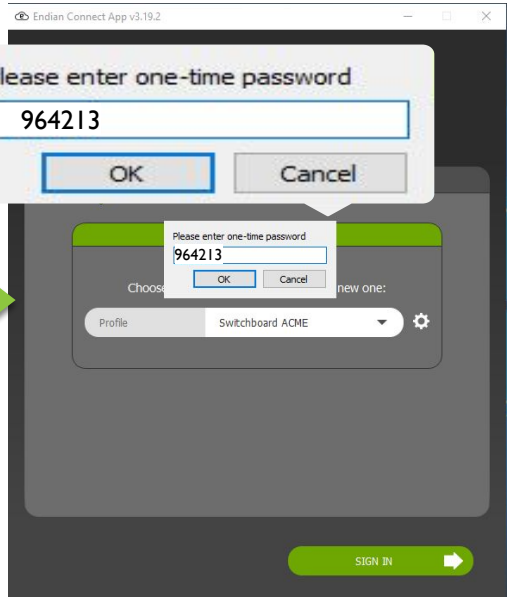
In order to authenticate to an Endian using 2FA, it's recommended to use the Endian Connect App client. Under the settings for your specified connection, check the box to enable OTP and once you click "Sign In" you will be prompted to enter your OTP token.

endian
Secure everyThing

Module
VPN

2-Factor VPN Authentication

Using Endian Connect App



endian
Secure everyThing

Module
VPN

2-Factor VPN Authentication

Using Third-Party VPN Applications

In order to authenticate to an Endian using 2FA, using a third-party OpenVPN client, enter in your client password field your password followed by a space (␣) and then enter the OTP token displayed on your mobile device.

Example: with password **MyPass123+** and token **123456**, you'll enter "**MyPass123+␣123456**" in the password field

** You can use any OpenVPN client to connect to Endian using 2FA and the same procedure for the password field*

endian
Secure everyThing

Module
VPN

2-Factor VPN Authentication

Using Third-Party VPN Applications

endian
Secure everyThing

Module
VPN

OpenVPN Demo

endian

Secure everyThing

Thanks

End :: SSL VPN (OpenVPN)

endian ESAT