TREND MICRO™

2.5 Deep Edge™ Service Pack 2 Deployment Guide

Next Generation Firewall Protection

Network Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/home.aspx

Document Part No.: CTEM26693_140930

Release Date: November 2014

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available in the Trend Micro Online Help and/or the Trend Micro Knowledge Base at the Trend Micro website.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Table of Contents

About This Manual

Chapter 1: Deep Edge Next Generation Firewall

Chapter 2: Deployment Planning

Chapter 3: Deep Edge Deployment

Chapter 4: Security Policy Configuration

Appendix A: Technical Support

Index

Preface

About This Manual

Welcome to the Trend Micro™ Deep Edge™ 2.5 Deployment Guide. This guide explains the Deep Edge appliance deployment modes and initial policy configurations. It also describes post-upgrade configurations, testing the installation, troubleshooting, and accessing Technical Support.

Topics include:

Deep Edge Documentation

The documentation set for Deep Edge includes the following:

TABLE 1. Deep Edge Document Set

DOCUMENT	DESCRIPTION
Administrator's Guide	This guide provides detailed information about the Deep Edge next-generation firewall configuration options. Topics include managing updates to stay protected against the latest risks, using policies to support security objectives, configuring scanning and URL filtering, and understanding logs and reports.
Deployment Guide	This guide explains the Deep Edge appliance deployment modes and initial policy configurations. It also describes post-upgrade configurations, testing the installation, troubleshooting, and accessing Technical Support.
Quick Start Guide	This guide gives information about unpacking, setting up, and logging into a new Deep Edge appliance.
Online Help	The online help provides the same content as the *Administrator's Guide* and is accessible from the Deep Edge web console.
Readme File	This file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and, release history.
Knowledge Base	The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to: http://esupport.trendmicro.com/

DOCUMENT	DESCRIPTION
TrendEdge	TrendEdge provides Trend Micro employees, partners, and other interested parties with information about unsupported, innovative techniques, tools, and best practices for Trend Micro products. The TrendEdge database contains numerous documents covering a wide range of topics. To access TrendEdge, go to: http://trendedge.trendmicro.com

The latest versions of the documentation is available in electronic form at:

http://docs.trendmicro.com/en-us/home.aspx/

Audience

The Deep Edge documentation is written for IT managers and system administrators working in enterprise environments. The documentation assumes that the reader has in-depth knowledge of network schemas and network fundamentals.

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output

CONVENTION	DESCRIPTION
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions
 **Important**	Information regarding required or default configuration settings and product limitations
 **WARNING!**	Critical actions and configuration options

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

Chapter 1

Deep Edge Next Generation Firewall

Topics include:

Deep Edge Overview

Deep Edge offers a new level of simplicity for deployment, configuration, and management of a next-generation firewall solution. Its all-functions-turned-on high performance scanning intelligently protects the network, endpoint, and server environments from web, email, and other network-based malicious activity including viruses, worms, spyware, bots, Trojans and phishing scams. Deep Edge also offers VPN connectivity to secure connections from mobile devices, corporate sites, and remote employees. All advanced security capabilities are easily configured, deployed, and viewed on an intuitive and flexible web-based console.

What's New

TABLE 1-1. New Features in Deep Edge 2.5 Service Pack 2

FEATURE	DESCRIPTION
Setup Wizard	The Deep Edge Setup Wizard provides a step-by-step interface to configure and deploy the Deep Edge appliance. The Setup Wizard enhances the configuration flow by providing contextual information about each configuration to help system administrators make informed decisions about the deployment. The Setup Wizard automatically initiates after logging on the appliance for the first time. Access the Setup Wizard by clicking **Wizard** from the web console's top menu.

Feature	Description
Network Diagnostics	The Network Diagnostics tool helps troubleshoot common connectivity issues, including: • Internet access • DNS configuration • Traffic routing • Trend Micro ActiveUpdate access • Trend Micro Web Reputation Service (WRS) access Access the Network Diagnostics tool by clicking **Network Diagnostics** from the web console's top menu.
Integration with Deep Discovery Inspector	Configure Deep Discover Inspector integration as part of an advanced anti-malware protection strategy. Trend Micro Deep Discovery Inspector is a separately licensed product that provides advanced network monitoring and threat intervention. With 360-degree monitoring of network traffic, Deep Discovery Inspector provides network-wide visibility and intelligence to detect and respond to targeted attacks. Deep Discovery Inspector enables administrators to select, create, configure, import, and export IP addresses, URLs, and domains as lists of denied or allowed objects. Deep Discovery Inspector can also add IP addresses, URLs, and domains from Virtual Analyzer feedback or from behavior or pattern matching scans. Deep Edge uses the Deep Discovery Inspector deny lists to block connections from denied IP addresses, URLs, and domains.

Feature	Description
Policy validation and checking	Deep Edge enhances policies by validating already configured policies to help system administrators configure policies that do not conflict in how they route traffic. Policy checking also assists system administrators in configuring policies as they are intended by highlighting any potentially conflicting configuration in policies with a higher priority than the configured policy.

Table 1-2. New Features in Deep Edge 2.5 Service Pack 1

Feature	Description
Advanced anti-malware protection	The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and aggressive heuristic scanning to detect document exploits and other threats used in targeted attacks.
Integration with Deep Discovery Advisor	Trend Micro™ Deep Discovery Advisor is a separately licensed product that provides unique security visibility based on Trend Micro's proprietary threat analysis and recommendation engines. Deep Edge integrates with the Virtual Analyzer in Deep Discovery Advisor.
Streamlined network configuration	To simplify network configurations, Deep Edge streamlines the settings for interfaces, DNS, DHCP and DNS forwarding, and bridged interfaces.

TABLE 1-3. New Features in Deep Edge 2.5

FEATURE	DESCRIPTION
Dual ISP and WAN support	Deep Edge can now support dual WAN or ISP connections. • In routing mode, Deep Edge 2.5 extends static and dynamic routing with policy-based routing using the destination or source IP address, the service type, or the egress interface of multiple ISPs or WANs. For details, see *About Policy-based Route Management on page 3-14*. • In bridge mode, Deep Edge 2.5 supports multiple bridged interfaces. For details, see *Bridging Interfaces on page 3-11*.
Enhanced IPS performance	Deep Edge Intrusion Prevention Systems (IPS) performs deep content inspection on all traffic to stop harmful activities. Deep Edge 2.5 now has the capabilities to scan traffic with over 7000 easily-configured predefined IPS rules by setting filtering criteria about the severity level, affected operating systems, release date, or traffic categories.
Granular application control	Application control objects now include specific behaviors within the application, such as only limiting video calls or uploading files, to set granular policy rules.
New custom URL category objects	Deep Edge 2.5 supports customized URL category objects.
Command & Control (C&C) Contact Alert Services	Command & Control (C&C) Contact Alert Services provides Deep Edge with enhanced detection capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks by blocking traffic from high-risk sources. A new **C&C Callback Attempts** widget tracks advanced persistent threat activity in your network by providing actionable intelligence about the user, the compromised host, and how Deep Edge enforced policy actions.

Feature	Description
Improved widget framework	Several improvements to the widget framework have increased performance, reliability and speed of the dashboard widgets.
Increased configuration visibility	A new *Getting Started* guide is available to simplify the setup process. Access help content by going to **Administration** > **Getting Started** from the web console.
Improved NAT rules	Each Deep Edge 2.5 NAT rule now has a description parameter to easily differentiate between multiple SNAT and DNAT configurations.
More robust log analysis	Deep Edge 2.5 enhances log presentation in the dashboard, log query results, and reports.

Table 1-4. New Features in Deep Edge 2.1

Feature	Description
Bandwidth Control	Peer-to-peer downloading, video streaming and instant message applications consume network bandwidth and can impact productivity. Deep Edge 2.1 supports using bandwidth control to reduce network congestion by controlling communications, reducing unwanted traffic and allowing critical traffic or services the appropriate bandwidth allocation. In addition to policy settings, a new Bandwidth Control widget illustrates affected traffic.
VPN enhancements	Deep Edge 2.1 enhances VPN compatibility: • Total connected clients are now listed in the **Clients** tab • PPTP VPN now allows for a larger address pool • Address objects are now listed in the **Local Networks** drop-down list
Mobile VPN compatibility	Deep Edge 2.1 Mobile VPN supports multiple local domains.

Feature	Description
Local users and groups	Local user and group management allows for authentication when an organization does not use Active Directory or LDAP authentication. Additional Deep Edge 2.1 enhancements include: • Only authenticated local users can access the external network • Policy rules support local user and group selection • Local user management improvements • VPN support

Table 1-5. New Features in Deep Edge 2.0

Feature	Description
HTTPS Inspection	The HTTPS Inspection feature in Deep Edge allows you to enable or disable HTTPS inspections, configure client certificate requests, and exclude specific websites, URLs, and IP addresses from inspection.
Mobile VPN Support	Deep Edge, a gateway device, provides VPN services not only to laptops or desktops but also mobile devices. Mobile VPN offers support for mobile devices in the “closed” environment of Apple iOS or the “open source“ environment of Android.
Anti-DoS Capability (and Report)	Deep Edge prevents Denial of Service (DoS) or a Distributed Denial of Service (DDoS) attacks, which attempt to make a machine or network resource unavailable to users, and is intended to temporarily or indefinitely interrupt or suspend services to a host connected to the Internet. Typical attacks involve saturating the target machine with external communication requests, such that the machine can no longer respond to legitimate traffic or responds so slowly it is rendered unavailable. Such attacks usually lead to server overload.
End-user Notifications	Deep Edge provides end-user notifications for violations of the following policies: Web Reputation Services (WRS), URL Filtering, anti-malware, blacklisted URLs, file extensions detections, IPS and certificate failure (server and client).

Feature	Description
Email Security Solution	Deep Edge processes SMTP or POP3 email messages, scans them, and either cleans infected email messages and delivers them or performs the user-selected action set in the policy on email messages in violation. Email messages can be quarantined and delivered later.
SSL VPN Enhancements	Deep Edge supports Secure Sockets Layer Virtual Private Network (SSL VPN), a form of VPN that can be used with a standard Web browser. The Deep Edge SSL VPN solution requires the installation of client software, and is ideal for applications including web-based email, business and government directories, file sharing, remote backup, remote system management, and consumer-level electronic commerce.

Main Features

The tables below describe key parts of the Deep Edge solution. All technology components are designed to integrate and optimized performance, which allows all security features to be turned on while providing excellent product performance.

Security Protection

Feature	Description
Advanced Firewall	Easily deploy and manage next-generation firewall capabilities. The Advanced Firewall blocks attacks while allowing good application traffic to pass.
IPS/IDS	Identify and stop many active threats, exploits, back-door programs, and other attacks, including DoS and DDoS attacks, passing through the device. The Intrusion Prevention System and Intrusion Detection System (IPS/IDS) bolsters a firewall's security policy by ensuring that traffic allowed by the firewall is further inspected to make sure it does not contain unwanted threats.

Feature	Description
Web Protection	Use Trend Micro Web Reputation technology to control the level of protection against malicious websites.
Antivirus	Leverage multiple security components and antivirus protection based on high-speed application content scanning to protect the customer with lower latency and improved user experience.
Anti-spam	Use Trend Micro Email Reputation Services (ERS) and an integrated high speed anti-spam engine to detect, block, or quarantine spam email messages based on the reputation of the mail sender and the email content .
ActiveUpdate	Enable on-demand and real-time updates from the Smart Protection Network to the local virus, protocol, spyware, IPS, IntelliTrap, and anti-spam pattern files.

Operations Control

Feature	Description
Application Control	Automatically discover popular Internet applications and control access to them using policies.
URL Filtering	Create and configure unique URL filtering procedures for different profiles. URL filtering, along with WRS, is part of the multi-layered, multi-threat protection solution.
LDAP Integration	Integrate with Lightweight Directory Access Protocol (LDAP) including Active Directory and OpenLDAP, to create policies specific to users or groups. Event logs and reports use LDAP user names and groups for user identification.

Visibility and Monitoring

Feature	Description
Summary Dashboard	Customize the dashboard to select, drill down, and display security and traffic information using widgets.

Feature	Description
Application Bandwidth Monitoring	Record and monitor top bandwidth users on the network with Application Control and LDAP integration. Notify managers about abuse by identifying users and the applications used that burden the network.
System Notifications and Alerts	Send security-related event email notifications (alerts) for: • Firewall • Web Reputation Service (WRS) • Malware • Intrusion Protection Services (IPS) • Hardware monitoring • URL filtering • Application control violations Notifications are sent directly to end-users, allowing them to take corrective action without impacting IT administrators.
Reports	Generate reports about detected malware and malicious code, blocked files, and accessed URLs to optimize program settings and fine tune security policies.
Logs	Detect and act upon security risks according to the settings specified for each risk type. These events are recorded in the logs.

Network Connectivity

Feature	Description
Network Configuration	View and edit detected network interfaces, or modify physical L2 and L3 port configurations. The following configurations are support for L3 ports: • Dynamic Host Configuration Protocol (DHCP) • Static route configurations by IP address and netmask • Point-to-point Protocol over Ethernet (PPPoE)
Bridging	Transparently bridge two interfaces and filter network traffic to protect endpoints and servers with minimal impact to the existing network environment. Spanning Tree Protocol (STP) ensures a loop-free topology for any bridged Ethernet local area network.
Routing	Configure static and dynamic routes, including Routing Information protocol (RIP) and Open Path Shortest First (OSPF).
NAT	Configure Network Address Translation (NAT) policies to specify whether source or destination IP addresses and ports are converted between public and private addresses and ports.
Services	Configure the following services: • Domain Name server (DNS) forwarding • Dynamic Host Configuration Protocol (DHCP) servers • Dynamic DNS (DDNS) settings
User VPN	Configure Virtual Private Network (VPN) with the Point-to-Point Tunneling Protocol (PPTP), Secure Sockets Layer Virtual Private Network (SSL VPN).
Site-to-Site VPN	Create encrypted L3 tunnels by using the Internet Key Exchange (IKE) and IP Security (IPsec) protocols.

Feature	Description
Mobile VPN	Allow iPhone and Android mobile device users to easily and securely connect back to the corporate environment by utilizing the built-in IPsec VPN clients. No agent installation is required for the mobile devices.

Chapter 2

Deployment Planning

Topics include:

Web Browser Requirements

To access the HTTP-based web console, use any of the browsers listed in the following table.

TABLE 2-1. Supported Web Browsers for Web Console Access

BROWSER	WINDOWS		LINUX
	XP SP3	Windows 7	RHEL 5 Server
Internet Explorer 8, 9, 10	✔	✔	
Firefox 28+	✔	✔	✔
Google Chrome 29+		✔	✔

Proxy for Internet Updates

If you have a proxy host between Deep Edge and the Internet, you must configure the Deep Edge's proxy settings in order to receive security updates from Trend Micro. From the menu, go to **Administration** > **System Settings** > **Proxy Settings** to configure the upstream proxy settings.

Activation Codes

Deep Edge includes one registration key. During product registration, the Registration Key is exchanged for an Activation Code that "unlocks" the program. You can register the installation and exchange the registration key for an activation code from a link in the setup program. Alternatively, you can register and obtain an activation code before installing by visiting the Trend Micro online registration website at:

https://olr.trendmicro.com

Chapter 3

Deep Edge Deployment

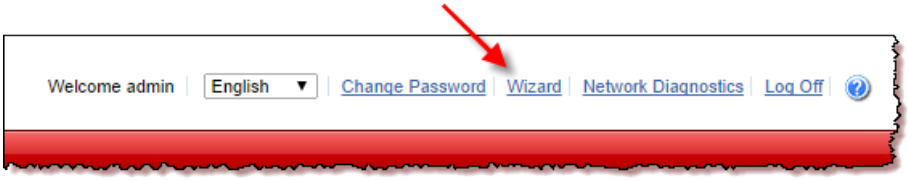
This chapter explains how to deploy Deep Edge in the Bridge, Routing, and Monitoring modes.

Topics include:

Setup Wizard

The Deep Edge Setup Wizard provides a step-by-step interface to configure and deploy the Deep Edge appliance. The Setup Wizard enhances the configuration flow by providing contextual information about each configuration to help system administrators make informed decisions about the deployment. The Setup Wizard automatically initiates after logging on the appliance for the first time.

Access the Setup Wizard by clicking **Wizard** from the web console's top menu.



About Deployment Modes

This section provides an overview of the working modes of Deep Edge, and how to configure Deep Edge for each mode.

Deep Edge runs in two different inline modes, depending on the network infrastructure and requirements. Use Routing mode and Bridge mode for traffic inspection and to take action based on policies. They support the same network security features. Use Monitoring mode to evaluate what effect security policies might have if deployed in Routing mode or Bridge mode.

TABLE 3-1. Deployment Modes

MODE	PURPOSE
Bridge	The Deep Edge unit is invisible to the network. All of its interfaces are on the same subnet. You only have to configure a management IP address so that you can make configuration changes. You would typically use Bridge mode on a private network behind an existing firewall or behind a router. For details, see *Overview of Bridge Mode on page 3-3*.
Routing	The Deep Edge unit is visible to the network. All of its interfaces are on different subnets. Each interface connected to a network must be configured with an IP address valid for that network. You would typically use Routing mode when the Deep Edge unit is deployed as a gateway between private and public networks. For details, see *Overview of Routing Mode on page 3-5*.
Monitoring	Monitoring mode is designed for evaluating Deep Edge on a production network without blocking any traffic or making Deep Edge a point of failure in the network flow. In Monitoring mode, Deep Edge only applies policies to mirrored traffic to produce logs and reports; no blocking actions are enforced on the traffic. For details, see *Overview of Monitoring Mode on page 3-7*.

Overview of Bridge Mode

In bridge mode, Deep Edge is invisible on the network and acts as a layer 2 bridge between network devices (switch, router, or firewall), transparently scanning network traffic in both directions. Bridge mode is the simplest way to deploy Deep Edge into an existing network topology and does not require client, router, or switch modifications.

Deep Edge acts as a "bump in the wire" and scans for malware. *Figure 3-1: Deep Edge in Bridge mode on page 3-4* illustrates Deep Edge in Bridge mode:

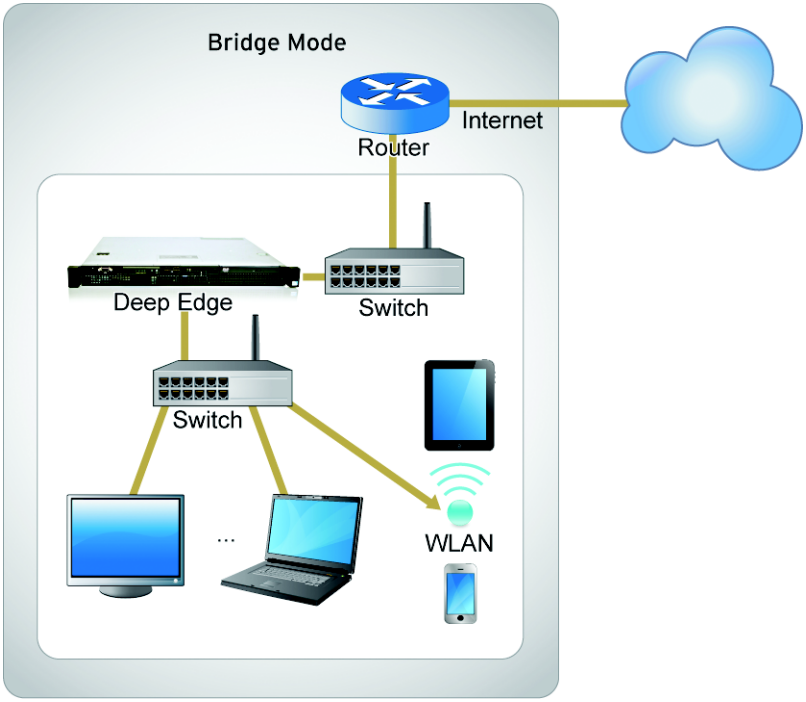


FIGURE 3-1. Deep Edge in Bridge mode

Similar to using a network bridge, all Deep Edge interfaces must be on the same subnet. To configure bridge mode, two network cards are required; one for internal use, and one for external use. You can also configure an IP address on the bridge to manage Deep Edge for scheduled pattern updates and to leverage the real-time security information power of the Trend Micro Smart Protection Network™ in the Cloud.

Configure bridge mode when Deep Edge operates on a private network behind an existing firewall or router so that Deep Edge can perform all scanning functions transparently.

For details about configuring bridge mode, see *Bridging Interfaces on page 3-11*.

Overview of Routing Mode

In routing mode, Deep Edge is visible on the network and acts as a layer 3 routing device with traffic stream scanning capabilities. Deploying in routing mode requires configuring two network interfaces: one for internal use and one for external use. All the interfaces are on different subnets, enabling you to have a single IP address available to the public Internet. Deep Edge can perform network address translation before it sends and receives packets to the destination network and works as a router.

Deep Edge also provides Point-to-Point Protocol over Ethernet (PPPoE) functionality to support dialing to the ISP through asymmetric digital subscriber line (ADSL). See the

following figure for the typical deployment. *Figure 3-2: Deep Edge in Routing Mode on page 3-6* illustrates Deep Edge in routing mode:

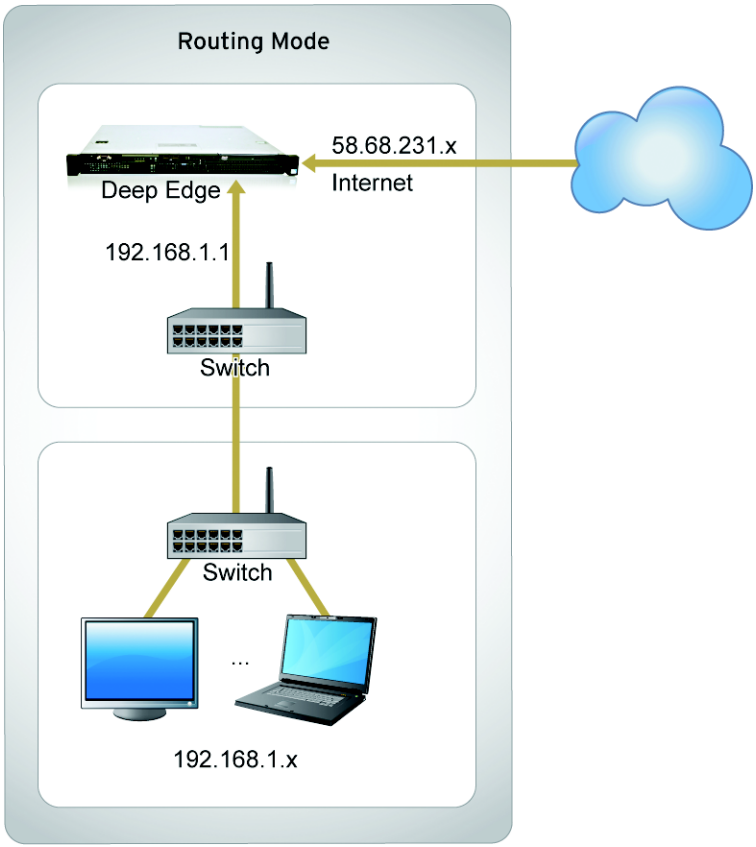


FIGURE 3-2. Deep Edge in Routing Mode

Configure routing mode when Deep Edge operates as a gateway between private and public networks. In this configuration, you must create NAT mode firewall policies to control traffic flow between the internal, private network and the external, public network, usually the Internet.

For details about configuring Routing mode, see *Routing Mode Configuration on page 3-14*.

Overview of Monitoring Mode

Monitoring mode is designed for evaluating Deep Edge on a production network without blocking any traffic or making Deep Edge a point of failure in the network flow. In monitoring mode, Deep Edge is invisible to the network. Establish the correct monitoring settings on the network switch to mirror traffic to the port that connects to Deep Edge. Deep Edge will apply policies to the mirrored traffic, but only logs violation-related information. Network traffic is never blocked by policies in this mode.

Figure 3-3: Deep Edge in Monitoring mode on page 3-8 illustrates Deep Edge in monitoring mode:

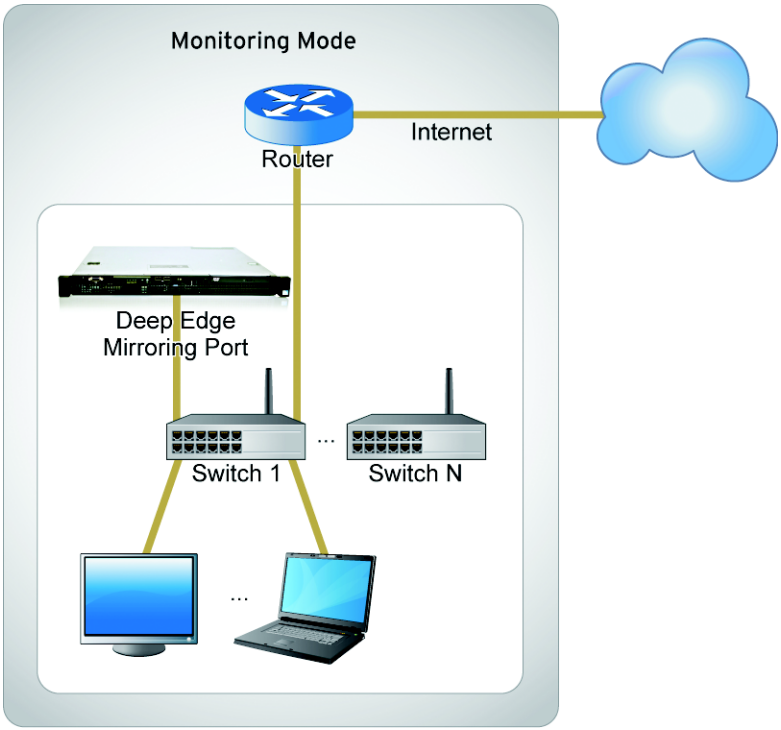


FIGURE 3-3. Deep Edge in Monitoring mode

In monitoring mode, network traffic does not pass directly through Deep Edge. Deep Edge runs independently outside the network (logically) aided by the switches of the network which mirror the specified traffic to interface(s) on which Deep Edge listens. Deep Edge monitors the status of the traffic and presents the information to the Deep Edge user.

Trend Micro suggests Deep Edge be deployed at the core Internet switch in order to see a copy of all Internet traffic leaving and entering the network. Deep Edge requires at least two network interfaces to function correctly in Monitoring mode. In addition to the interface that Deep Edge uses to listen for traffic, there should be another

connection for Deep Edge to access the Internet to connect to the ActiveUpdate and WRS query servers, as well as other cloud protection sources that Deep Edge offers.

Monitoring mode is typically used when:

- The network already has related devices (firewall, IDS/IPS) deployed, but there is a lack of visibility into the overall network posture. In this case, Deep Edge provides visibility without dramatically changing the network topology.
- Before deploying Deep Edge inline, Monitoring mode could help with the evaluation of the Deep Edge device. After learning the security benefits provided by Deep Edge, you could change from Monitoring mode to either Bridge mode or Router mode for true inline protection.

For details about configuring Monitoring mode, see *Monitoring Mode Configuration on page 3-18*.

Deployment Mode Configuration

Deep Edge requires you to configure your preferred deployment mode through the Deep Edge web console or user interface.

Connecting to the web-based manager requires:

- A computer with an Ethernet connection
- A compatible web browser
- An Ethernet cable

You can deploy Deep Edge in the following modes:

- *Routing Mode Configuration on page 3-14*
- *Bridging Interfaces on page 3-11*
- *Monitoring Mode Configuration on page 3-18*

Logging on to the Web Console

Log on to Deep Edge to set the deployment mode.

Procedure

1. Use the address `https://<appliance_IP_address>:8443`.

   Specify the IP address provided during the installation.

   Important

   Remember to include the "s" in `https://`

2. Specify the administrator credentials.

   Default credentials:

   User name: `admin`

   Password: `adminDeepEdge`

3. Press ENTER or click **Log On**.

Deployment Mode Settings

The following table explains the required and optional settings to configure bridge mode, monitoring mode, or routing mode. Use it as a reference to ensure that you configure all necessary settings.

SETTING	BRIDGE/MONITORING MODE	ROUTING MODE
Deployment mode	**Required**	**Required**
Bridge interfaces	**Required**	
Interfaces		**Required**
Source NAT		**Required**

SETTING	BRIDGE/MONITORING MODE	ROUTING MODE
Destination NAT		**Optional**
Routing		**Optional**

Bridging Interfaces

A bridge connects two interfaces using the same protocol to pass traffic transparently across the bridged interfaces. While in bridge mode, Deep Edge is invisible on the network and acts as a layer 2 bridge between network devices (switch, router, or firewall), transparently scanning network traffic in both directions.

Note

To receive security updates from Trend Micro, make sure that the management interface can access the Internet.

Deep Edge supports dual links to configure multiple WAN/ISPs connected to the appliance. Deep Edge has two inbound and two outbound links. Add multiple bridges to support multiple ISPs or WANs. Deep Edge is transparent between the two ISPs while an L3 router manages traffic.

Deep Edge supports Spanning Tree Protocol (STP) to ensure a loop-free topology for any bridged Ethernet local area network.

Dual Link Support

Bridge multiple interfaces to configure multiple WAN/ISPs connected to Deep Edge. In bridge mode, Deep Edge has two inbound and two outbound links. Deep Edge is transparent between the two ISPs while the L3 router manages traffic. The following illustration shows how to configure Deep Edge in bridge mode to handle two ISPs with an L3 router.

Adding a Bridge

For a bridge mode overview, see *Overview of Bridge Mode on page 3-3*.

Procedure

1. Go to **Network** > **Deployment** and verify that the **Inline Mode** radio button is selected.
2. Go to **Network** > **Bridge**.
3. Click **Add New**.

   The **Add/Edit Bridge** screen appears.
4. Specify a name for the network bridge.
5. From the **Interface 1** and **Interface 2** drop-down list boxes, select the interfaces to bridge.

> **Note**
>
> These bridged interfaces should correspond to the trusted and untrusted sides of the network so that data can pass between the Internet and internal systems.

6. Under **Bridge Binding IP Configuration**, specify the network settings.

> **Note**
>
> The bridge IP address, netmask, and default gateway are optional when other L3 interfaces are configured with access rights to the web console.

OPTION	DESCRIPTION
IPv4 address	Specify the IPv4 address. Example: 123.123.123.123
IPv4 netmask	Specify the IPv4 subnet mask. Example: 255.255.254.0
IPv4 default gateway	Specify the IPv4 default gateway. This settings is only required for WAN configurations. Example: 123.123.123.123

Option	Description
IPv6 address / prefix length	Specify the IPv6 settings. Example: 2001:db8:10ff::ae:44f2/8
IPv6 default gateway	Specify the IPv6 default gateway. This settings is only required for WAN configurations. Example: 2001:db8:10ff::ae:44f2/64 Example: 2001:db8:10ff::ae:44f2/64
Administrative access	Select which management services and traffic to allow (web console, ping, SSH, SNMP). These services originate from devices behind the Deep Edge appliance.

7. Configure **Advanced Settings**.
   - Ensure a loop-free topology for the bridged network by selecting **Enable Spanning Tree Protocol**.
   - Ensure that attached devices are aware of the link status in high availability networks by selecting **Enable Link Loss Forwarding**. For information about Link Loss Forwarding, see *Link Loss Forwarding on page 3-13*.
8. Click **Apply**.

Link Loss Forwarding

Link Loss Forwarding ensures high availability by disabling both bridged interfaces if one interface fails. Any failure along the signal link is passed through and can be seen by attached devices. When Link Loss Forwarding is disabled, a failure in one bridged interface does not disable the other interface and connected devices are unaware that the link is lost.

Deep Edge monitors and enables the interface once the bridged interface signal link restores.

Routing Mode Configuration

Configuring Deep Edge in routing mode involves defining interface addresses, default routes, and simple security policies.

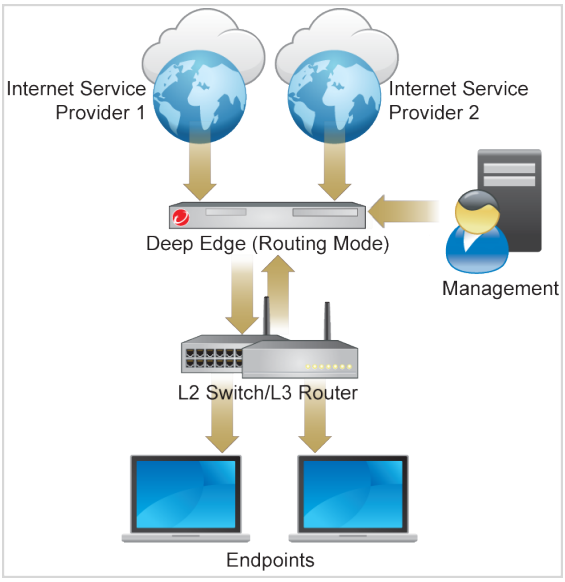
About Policy-based Route Management

In today's high performance networks, organizations need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional routing protocol concerns. While static and dynamic routing focus on the traffic destination for routing, policy-based routing provides a mechanism to mark packets so that certain kinds of traffic receive differentiated routing. Destination-based routing techniques make it difficult to change the routing behavior of specific traffic. Also known as “intelligent routing”, policy-based routing allows you to dictate the routing behavior based on a number of different criteria other than destination network, including source interface, source or destination address, or service type.

Consider a company that has two links between locations, one a high bandwidth, low delay expensive link and the other a low bandwidth, higher delay lower expense link. Using traditional routing protocols, the higher bandwidth link would get most if not all of the traffic sent across it based on the metric savings obtained by the bandwidth and/or delay (using EIGRP or OSPF) characteristics of the link. Policy-based routing can route higher priority traffic over the high bandwidth/low delay link while sending all other traffic over the low bandwidth/high delay link.

With policy-based routing, Deep Edge can route traffic from multiple ISPs and WANs. The following illustration shows how to configure Deep Edge for two ISPs using an L2 switch.

FIGURE 3-4. Policy-based Routing Example



Setting the Interface Type

Procedure

1. Go to **Network** > **Deployment** and verify that the **Inline Mode** radio button is selected.
2. Go to **Network** > **Interfaces**.
3. Do the following for each interface that corresponds to the trusted (internal) and untrusted side of the network. These interfaces will transmit data to and from the Internet and your internal systems.
   a. Click the name of the interface.

      The **Edit Interface** window appears.

   b. Set the interface type to **L3**.

c. Click **Apply**.

Connecting with PPPoE

For the interface that connects to the Internet, you can use PPPoE if you need to dial in to an Internet Service Provider (ISP).

Procedure

1. Go to **Network** > **Interfaces**.
2. Click the interface name that connects to the ISP.

   The **Edit Interface** window appears.

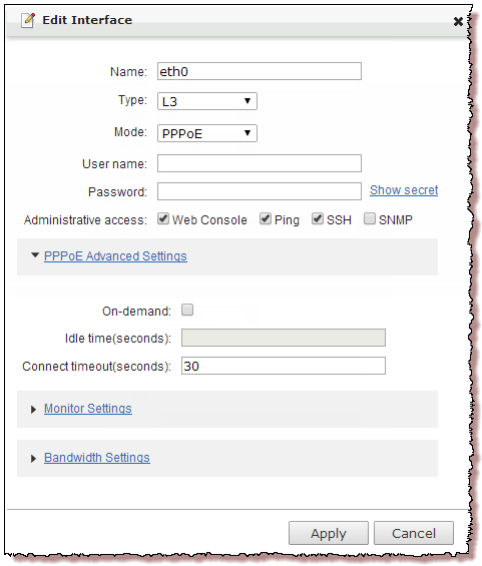


FIGURE 3-5. Configure the interface for Router mode

3. Configure the PPPoE settings.

Option	Description
Type	Select **L3**.
Mode	Select **PPPoE**.
User name	Specify the user name provided by the Internet Service Provider.
Password	Specify the password provided by the Internet Service Provider.
Administrative access	Select which management services (or traffic) to allow. These services originate from devices behind the Deep Edge appliance.
PPPoE Advanced Settings	Specify the on-demand, idle time, and connection timeout settings.

4. Click **Apply**.
5. Configure any other interfaces connected to the internal network.
6. To test the configuration, access an Internet website from an internal client.

Configuring the NAT

Procedure

1. Go to **Network** > **NAT**.
2. Click **Add New**.

The **Add/Edit NAT Rules** window appears.

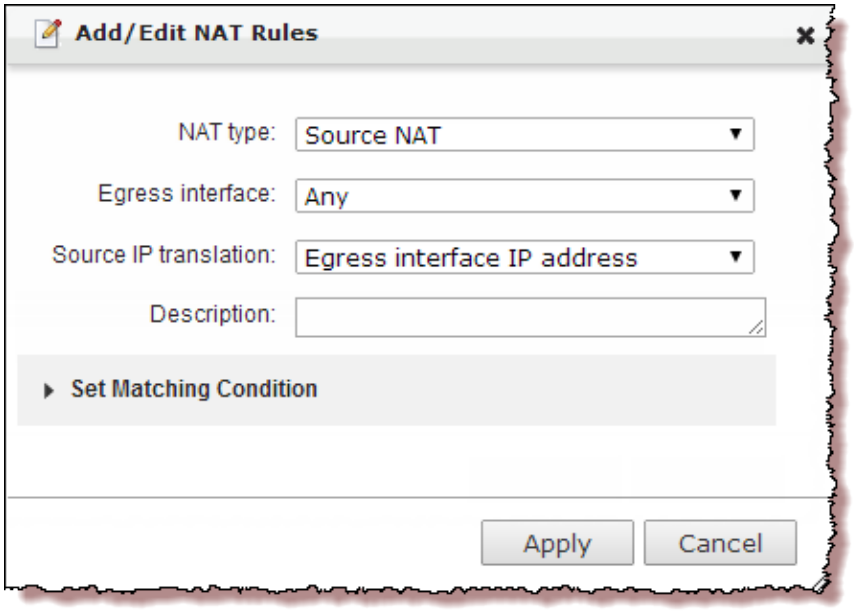


FIGURE 3-6. Configure the NAT settings to allow Deep Edge to connect

3. Configure the NAT to allow the connection to function correctly.

Monitoring Mode Configuration

Deploying Deep Edge in Monitoring mode is used mostly for evaluation. It requires some settings on the switch to mirror all the traffic to a port.

Deep Edge requires at least two network interfaces to function correctly in this mode. Establish the settings for your route and mirror the traffic to the port that connects to the Deep Edge. Deep Edge will monitor the network traffic and log any violation-related information.

Note

Be aware that:

- The management interface cannot be selected as the listening interface.
- Deep Edge will not block traffic in Monitoring mode. It cannot enforce security policies or act on blacklisted URLs.

Configuring Monitoring Mode

Before you begin

Before configuring Deep Edge in Monitoring mode:

- Determine which interface will receive traffic for monitoring.
- Mirror all traffic to a port on the core Internet switch.
- Connect the designated Deep Edge interface to the switch port.

Procedure

1. Log on to the Deep Edge web console.
2. Go to **Network** > **Deployment**.
3. Select the **Monitoring mode** radio button.

   The network interfaces appear.
4. In the right-side box, find the appropriate interface and click **+** to add the interface.

   The interface moves to the left-side box.
5. Click **Apply**.

   Deep Edge is now monitoring the selected interfaces.

Specifying a Default Static Route and NAT

Static routes control how traffic moves between endpoints connected to the network. Defining a static route provides Deep Edge with the information to forward a packet to

a particular destination. Configure static routes by defining the destination IP address and netmask of packets that the Deep Edge appliance is intended to intercept, and by specifying a gateway IP address for those packets. The gateway address specifies the next-hop router to which traffic will be routed.

Note

You must configure a default route for routing traffic or querying web reputation in the cloud or doing security update. Both bridge mode and routing mode use the default route.

Environments utilizing DHCP or PPPoE to access the Internet may not be required to configure DNS settings or the default static route.

Procedure

1. Log on to the Deep Edge web console.
2. Go to **Network** > **Routing** > **Static Routes**.
3. Click **Add New** to add a default route.

   The **Add/Edit Static Route** window appears.
4. Select **Enable static route**.
5. In the **Network** field, specify `0.0.0.0/0` as the network.
6. In the **Next hop** field, specify the default gateway IP address.
7. Click **Apply**.

   The new route appears in the static routes list.

You have now added a default route for Deep Edge.

Deep Edge provides two NAT modes: Source NAT and Destination NAT.

Configuring DNS Settings

Procedure

1. Log on to the Deep Edge web console.
2. Go to **Network** > **DNS**.
3. For either or both the **IPv4** and **IPv6** tabs, configure the DNS server IP addresses.

   Note

   If Deep Edge dynamically acquires the DNS from an Internet Service Provider, the **Inherit DNS Information** section appears with read-only DNS information.

4. Click **Apply**.

Changing the Management IP Address

Deep Edge is preconfigured with the default management interface (eth0) IP address set to `192.168.252.1`. Depending on your network, you may need to change the management IP address to connect the management interface to the network. The following procedure explains how to change the Deep Edge management IP address.

Procedure

1. Go to **Network** > **Interfaces** to view all Deep Edge network interfaces.
2. Under the **Name** column, click **eth0**.
3. Configure the static address settings.

OPTION	DESCRIPTION
Type	Select **L3**.
Mode	Select **Static**.

Option	Description
IPv4 address	Specify the IPv4 address. Example: 123.123.123.123
IPv4 netmask	Specify the IPv4 subnet mask. Example: 255.255.254.0
IPv4 default gateway	Specify the IPv4 default gateway. This settings is only required for WAN configurations. Example: 123.123.123.123
IPv6 address / prefix length	Specify the IPv6 settings. Example: 2001:db8:10ff::ae:44f2/8
IPv6 default gateway	Specify the IPv6 default gateway. This settings is only required for WAN configurations. Example: 2001:db8:10ff::ae:44f2/64
Administrative access	Select which management services and traffic to allow (web console, ping, SSH, SNMP). These services originate from devices behind the Deep Edge appliance.

4. Click Apply.

Chapter 4

Security Policy Configuration

After configuring the Deep Edge deployment mode, you must set up security policies to verify the deployment. Policy rules are based on traffic source and destination to monitor, tag, or block the network. In Routing and Bridge modes, use the traffic source and destination zones (interface) for the policy rules. In Monitoring mode, because there is only one interface, use an IP range for policy rules. Refer to the following table for details about how policy rules are applied to zones:

Topics include:

Security Policy Rules

The following table explains the security policy rules for internal, external and DMZ traffic.

Traffic Source/ Destination	Policy Application
Internal	An IP range (address), an interface (zone), or a user name (LDAP) making a connection inside the organization.
External	An interface (zone) making a connection outside the organization or to the Internet.
De-Militarized Zone (DMZ)	An interface (zone) connecting to the DMZ network. The DMZ contains specific servers, web/FTP servers, VPN servers, and email servers defined by the organization.

Note

You can optionally set up the user identification method to identify and set user-based policies. For details about integrating Deep Edge with an LDAP server for user identification, refer to the *Deep Edge Administrator's Guide*.

Security Policies for Bridge Mode

You will need to create specific zones for internal and external traffic based on the available interfaces.

See the following procedures:

- *Creating the Internal Security Policy in Bridge Mode on page 4-3*
- *Creating the External Security Policy in Bridge Mode on page 4-4*

After completing these procedures, you can safely route live network traffic through Deep Edge.

Creating the Internal Security Policy in Bridge Mode

Use this policy to scan all outgoing traffic.

Procedure

1. Log on the Deep Edge web console.

   For more information, see *Logging on to the Web Console on page 3-10*.

2. Go to **Policies** > **Rules** > **Add New**.

3. Specify a name and description for the new policy rule.

   > **Note**
   > New policies are automatically enabled.

4. To create the security policy:

   a. On the **Sources and Users** tab, select **Enable source zone rules**, select the **Selected** radio button, click **Add New**, and then create an "internal" zone with the appropriate interface.

   b. On the **Destinations** tab, select **Enable destination zone rules**, and then select **Any**

   c. On the **Schedule and Action Profile** tab, do the following:

      i. Select **Add New** from the **Action Profile** drop-down list.

         The **Add/Edit** window appears.

      ii. Specify a name and description for the object.

      iii. Select the following security functions and set their actions:

TABLE 4-1. Add Action Profile

NAME	ACTION
IPS	Monitor

NAME	ACTION
Anti-malware	Block
Anti-spam	Monitor
WRS	Block

iv. Click **OK** to save the new action profile.

5. Click **OK** to save the policy.
6. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Creating the External Security Policy in Bridge Mode

Use this policy to scan all incoming HTTP, FTP, and SMTP traffic.

Procedure

1. Go to **Policies** > **Rules** > **Add New**.
2. Specify a name and description for the new policy rule.

Note

New policies are automatically enabled.

3. To create the security policy:
   a. On the **Sources and Users** tab, select **Enable source zone rules** and then select **Any**.
   b. On the **Destinations** tab, select **Enable destination zone rules**, select the **Selected zones** radio button, click **Add New**, and then create an "external" zone with the appropriate interface.
   c. On the **Traffic Type** tab, select **Enable service rules**, select the **Selected** radio button, and then select **HTTP**, **FTP**, and **SMTP**.
   d. On the **Schedule and Action Profile** tab, do the following:

i. Select **Add New** from the **Action Profile** drop-down list.

The **Add/Edit** window appears.

ii. Specify a name and description for the object.

iii. Select the following security functions and set their actions:

TABLE 4-2. Add Action Profile

NAME	ACTION
IPS	Monitor
Anti-malware	Block
Anti-spam	Tag

4. Click **OK** to save the policy.

5. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Security Policies for Routing Mode (with DMZ)

During security policy configuration, specify zones for "Internal" and "External" based on the available interfaces. You can also set a zone for the De-Militarized Zone (DMZ), if needed.

If you have a DMZ, go to **Policies** > **Rules** > **Add New** and add five policies for the DMZ.

See the following procedures:

- *Creating the First Security Policy for Routing Mode (with DMZ) on page 4-6*
- *Creating the Second Security Policy for Routing Mode (with DMZ) on page 4-7*
- *Creating the Third Security Policy for Routing Mode (with DMZ) on page 4-9*
- *Creating the Fourth Security Policy for Routing Mode (with DMZ) on page 4-10*
- *Creating the Fifth Security Policy for Routing Mode (with DMZ) on page 4-12*

After creating all five policies, you can safely route live network traffic through Deep Edge.

Creating the First Security Policy for Routing Mode (with DMZ)

Use this policy to scan external network access to DMZ servers, including HTTP, FTP, and SMTP traffic. WRS is disabled to protect DMZ servers.

Procedure

1. Log on the Deep Edge web console.

   For more information, see *Logging on to the Web Console on page 3-10*.

2. Go to **Policies** > **Rules** > **Add New**.

3. Specify a name and description for the new policy rule.

   Note

   New policies are automatically enabled.

4. To create the security policy:

   a. On the **Sources and Users** tab, select **Enable source zone rules** and then select **Any**.

   b. On the **Destinations** tab, select **Enable destination zone rules**, select the **Selected zones** radio button, and then specify the "DMZ" zone with the appropriate interface.

Note

To add a new zone object, do the following:

i. Click **Add New**.

ii. Specify a name and description for the object.

iii. Click the **+** icon in the **Interfaces** table to select an interface.

iv. Click **OK**.

c. On the **Traffic Type** tab, select **Enable service rules**, select the **Selected** radio button, and then select **HTTP**, **FTP**, and **SMTP** from the list.

d. On the **Schedule & Action Profile** tab, do the following:

i. Select **Add New** from the **Action Profile** drop-down list.

The **Add/Edit** window appears.

ii. Specify a name and description for the object.

iii. Select the following security functions and set their actions:

TABLE 4-3. Add Action Profile

NAME	ACTION
IPS	Monitor
Anti-malware	Block
Anti-spam	Tag

5. Click **OK** to save the policy.

6. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Creating the Second Security Policy for Routing Mode (with DMZ)

Use this policy to scan external network requests from DMZ servers, including web servers, Windows update, or SMTP traffic.

Procedure

1. Go to **Policies** > **Rules** > **Add New**.
2. Specify a name and description for the new policy rule.

   Note

   New policies are automatically enabled.

3. To create the security policy:

   a. On the **Sources and Users** tab, select the **Enable source zone rules** check box, select the **Selected** radio button, and then select the "DMZ" zone that was created in *Creating the First Security Policy for Routing Mode (with DMZ) on page 4-6*.

   b. On the **Destinations** tab, select **Enable destination zone rules**, select the **Selected zones** radio button, and then specify the "External" zone with the appropriate interface.

   Note

   To add a new zone object, do the following:

   i. Click **Add New**.

   ii. Specify a name and description for the object.

   iii. Click the **+** icon in the **Interfaces** table to select an interface.

   iv. Click **OK**.

   c. On the**Traffic Type** tab, select **Enable service rules**, select the **Selected** radio button, and then select **HTTP**, **FTP**, and **SMTP** from the list.

   d. On the **Schedule & Action Profile** tab, do the following:

   i. Select **Add New** from the **Action Profile** drop-down list.

   The **Add/Edit** window appears.

   ii. Specify a name and description for the object.

iii. Select the following security functions and set their actions:

TABLE 4-4. Add Action Profile

NAME	ACTION
IPS	Monitor
Anti-malware	Block
Anti-spam	Monitor
WRS	Block

4. Click **OK** to save the policy.
5. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Creating the Third Security Policy for Routing Mode (with DMZ)

Use this policy to protect internal network access to DMZ servers.

Procedure

1. Go to **Policies** > **Rules** > **Add New**.
2. Specify a name and description for the new policy rule.

> **Note**
> New policies are automatically enabled.

3. To create the security policy:
   a. On the **Source & Users** tab, select the **Enable source zone rules** check box, select the **Selected** radio button, click **Add New**, and create an "Internal" zone with the appropriate interface.

Note

To add a new zone object, do the following:

i. Click **Add New**.

ii. Specify a name and description for the object.

iii. Click the **+** icon in the **Interfaces** table to select an interface.

iv. Click **OK**.

b. On the **Destinations** tab, select the **Enable destination zone rules** check box, select the **Selected zones** radio button, and then select the "DMZ" zone with the appropriate interface.

c. On the **Schedule & Action Profile** tab, do the following:

i. Select **Add New** from the **Action Profile** drop-down list.

The **Add/Edit** window appears.

ii. Specify a name and description for the object.

iii. Select the following security functions and set their actions:

TABLE 4-5. Add Action Profile

NAME	ACTION
IPS	Monitor
Anti-malware	Block

4. Click **OK** to save the policy.

5. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Creating the Fourth Security Policy for Routing Mode (with DMZ)

Use this policy to protect internal network access the external network.

Procedure

1. Go to **Policies** > **Rules** > **Add New**.
2. Specify a name and description for the new policy rule.

   Note

   New policies are automatically enabled.

3. To create the security policy:

   a. On the **Source tab**, select **Enable source zone rules**, select the **Selected zones** radio button, and then select an "Internal" zone with the appropriate interface.

   b. On the **Destination tab**, select **Enable destination zone rules**, select the **Selected zones** radio button, and then select an "External" zone with the appropriate interface

   c. On the **Schedule & Action Profile** tab, do the following:

      i. Select **Add New** from the **Action Profile** drop-down list.

      The **Add/Edit** window appears.

      ii. Specify a name and description for the object.

      iii. Select the following security functions and set their actions:

      TABLE 4-6. Add Action Profile

NAME	ACTION
IPS	Monitor
Anti-malware	Block
Anti-spam	Monitor
WRS	Block

4. Click **OK** to save the policy.

5. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Creating the Fifth Security Policy for Routing Mode (with DMZ)

Use this policy to block all access from an external zone to internal zone.

Procedure

1. Go to **Policies** > **Rules** > **Add New**.
2. Specify a name and description for the new policy rule.

   Note
   New policies are automatically enabled.

3. To create the security policy:
   a. On the **Sources and Users** tab, select **Enable source zone rules** and then select **Any**.
   b. On the **Destinations** tab, select **Enable destination zone rules** and then select **Any**.
   c. On the **Schedule & Action Profile** tab, do the following:
      i. Select **Add New** from the **Action Profile** drop-down list.

         The **Add/Edit** window appears.

      ii. Specify a name and description for the object.
      iii. Select the following security functions and set their actions:

TABLE 4-7. Add Action Profile

NAME	ACTION
IPS	Block

NAME	ACTION
Anti-malware	Block
Anti-spam	Block
WRS	Block

4. Click **OK** to save the policy.
5. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Security Policies for Routing Mode (without DMZ)

If you do not have a DMZ, you must create at least two security policy rules for outbound and inbound traffic.

See the following procedures:

- *Creating the First Security Policy for Routing Mode (without DMZ) on page 4-13*
- *Creating the Second Security Policy for Router Mode (without DMZ) on page 4-15*

After completing these procedures, you can safely route live network traffic through Deep Edge.

Creating the First Security Policy for Routing Mode (without DMZ)

Use this policy to scan all outgoing traffic. All requests from internal endpoints match the policy rule.

Procedure

1. Log on the Deep Edge web console.

For more information, see *Logging on to the Web Console on page 3-10*.

2. Go to **Policies** > **Rules** > **Add New**.

3. Specify a name and description for the new policy rule.

> **Note**
> New policies are automatically enabled.

4. To create the security policy:

   a. On the **Sources and Users** tab, select the **Enable source zone rules** check box, select the **Selected** radio button, and then specify an "Internal" zone with the appropriate interface.

   > **Note**
   > To add a new zone object, do the following:
   >
   > i. Click **Add New**.
   >
   > ii. Specify a name and description for the object.
   >
   > iii. Click the **+** icon in the **Interfaces** table to select an interface.
   >
   > iv. Click **OK**.

   b. On the **Destinations** tab, select **Enable destination zone rules**, select the **Selected zones** radio button, and then specify an "External" zone with the appropriate interface.

   > **Note**
   > To add a new zone object, do the following:
   >
   > i. Click **Add New**.
   >
   > ii. Specify a name and description for the object.
   >
   > iii. Click the **+** icon in the **Interfaces** table to select an interface.
   >
   > iv. Click **OK**.

   c. On the **Schedule & Action Profile** tab, do the following:

i. Select **Add New** from the **Action Profile** drop-down list.

The **Add/Edit** window appears.

ii. Specify a name and description for the object.

iii. Select the following security functions and set their actions:

TABLE 4-8. Add Action Profile

NAME	ACTION
IPS	Monitor
Anti-malware	Block
Anti-spam	Monitor
WRS	Block

5. Click **OK** to save the policy.

6. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Creating the Second Security Policy for Router Mode (without DMZ)

Use this policy to scan external network access. For example, when an external email server sends content to an internal Microsoft Exchange server. Enabled traffic includes HTTP, SMTP and FTP only.

Procedure

1. Log on the Deep Edge web console.

   For more information, see *Logging on to the Web Console on page 3-10*.

2. Go to **Policies** > **Rules** > **Add New**.

3. Specify a name and description for the new policy rule.

Note

New policies are automatically enabled.

4. To create the security policy:

   a. On the **Sources and Users** tab, select **Enable source zone rules**, select the **Selected** radio button, and then specify an "External" zone with the appropriate interface.

   b. On the **Destinations** tab, select **Enable destination zone rules**, select the **Selected zones** radio button, and then specify an "Internal" zone with the appropriate interface.

   c. On the**Traffic Type** tab, select **Enable service rules**, select the **Selected** radio button, and then select **HTTP**, **FTP**, and **SMTP** from the list.

   d. On the **Schedule & Action Profile** tab, do the following:

      i. Select **Add New** from the **Action Profile** drop-down list.

      The **Add/Edit** window appears.

      ii. Specify a name and description for the object.

      iii. Select the following security functions and set their actions:

TABLE 4-9. ADD ACTION PROFILE

NAME	ACTION
IPS	Monitor
Anti-malware	Block
Anti-spam	Monitor

5. Click **OK** to save the policy.

6. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Security Policies for Monitoring Mode

You will need to create an address object and two security polices for Monitoring mode.

See the following procedures:

- *Creating the Internal Security Policy for Monitoring Mode on page 4-17*
- *Creating the External Security Policy for Monitoring Mode on page 4-18*

After completing these procedures, you can safely mirror live network traffic through Deep Edge.

Creating the Internal Security Policy for Monitoring Mode

Use this policy to scan all outgoing traffic.

Procedure

1. Go to **Policies** > **Rules** > **Add New**.
2. Specify a name and description for the new policy rule.

   Note

   New policies are automatically enabled.

3. To create the security policy:

   a. On the **Source & Users** tab, select the **Selected addresses** radio button under the **Source Address**, and then select an "Internal" address object from the **Name** column.

Note

To add a new address object, do the following:

i. Click **Add New**.

ii. Specify a name and protocol for the object.

iii. Specify an IP address or range of addresses in the **IP Address** field.

iv. Click **OK**.

b. On the **Destinations** tab, select the **Any** radio button under the **Destination Address.**

c. On the **Schedule & Action Profile** tab, do the following:

i. Select **Add New** from the **Action Profile** drop-down list.

The **Add/Edit** window appears.

ii. Specify a name and description for the object.

iii. Select the following security functions and set their actions:

TABLE 4-10. Add Action Profile

NAME	ACTION
IPS	Monitor
Anti-malware	Monitor
Anti-spam	Monitor
WRS	Monitor

4. Click **OK** to save the policy.

5. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Creating the External Security Policy for Monitoring Mode

Use this policy to scan all incoming HTTP, FTP, and SMTP traffic.

Procedure

1. Go to **Policies** > **Rules** > **Add New**.
2. Specify a name and description for the new policy rule.

Note

New policies are automatically enabled.

3. To create the security policy:
   a. On the **Source & Users** tab, select the **Any** radio button for **Source Address**.
   b. On the **Destinations** tab, select the **Selected** radio button under **Destination Address**, and then select an "Internal" address object from the **Name** column.

Note

To add a new address object, do the following:

i. Click **Add New**.
ii. Specify a name and protocol for the object.
iii. Specify an IP address or range of addresses in the **IP Address** field.
iv. Click **OK**.

   c. On the **Traffic Type** tab, select **Enable service rules**, select the **Selected** radio button, and then select **HTTP**, **FTP**, and **SMTP**.
   d. On the **Schedule & Action Profile** tab, do the following:
      i. Select **Add New** from the **Action Profile** drop-down list.

         The **Add/Edit** window appears.

      ii. Specify a name and description for the object.
      iii. Select the following security functions and set their actions:

TABLE 4-11. Add Action Profile

NAME	ACTION
IPS	Monitor
Anti-malware	Monitor
Anti-spam	Monitor

4. Click **OK** to save the policy.
5. Above the list of security policies, click **Apply** to apply the policy to current traffic.

Changing the Default Policy Priority

Deep Edge security policy priority is based on the policy order. For other policy rules to apply, move the default policy to the bottom of available policies.

Procedure

1. Go to **Policies** > **Rules** .
2. Select the policy named **Default** from the list and then click **Bottom**.

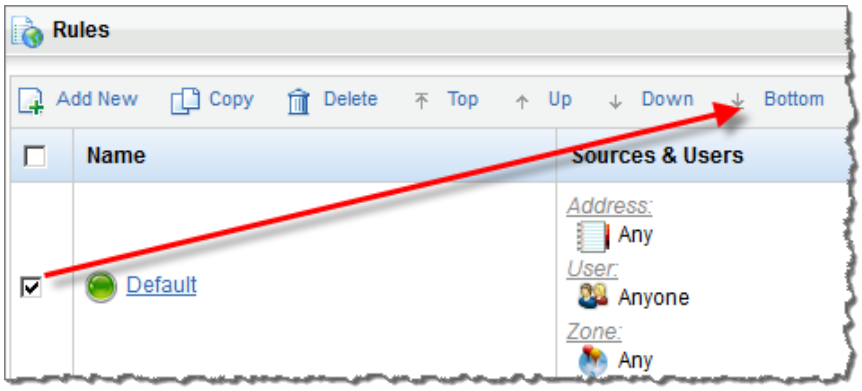


FIGURE 4-1. Changing Default Policy Priority

The default policy moves to lowest priority.

Appendix A

Technical Support

This appendix describes how to find solutions online, use the Support Portal, and contact Trend Micro.

Topics include:

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

http://community.trendmicro.com/

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select a product or service from the appropriate drop-down list and specify any other related information.

   The **Technical Support** product page appears.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Security Intelligence Community

Trend Micro cyber-security experts are an elite security intelligence team specializing in threat detection and analysis, cloud and virtual security, and data encryption.

Go to http://www.trendmicro.com/us/security-intelligence/index.html to learn about:

- Trend Micro blogs, Twitter, Facebook, YouTube, and other social media
- Threat reports, research papers, and spotlight articles
- Solutions, podcasts, and newsletters from global security insiders
- Free tools, apps, and widgets.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass endpoint security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://www.trendmicro.com/vinfo to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports.

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone, fax, or email:

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Record the case number for tracking purposes.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1036097.aspx

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

http://trendedge.trendmicro.com/

Known Issues

Known issues are features in your the product or software that might temporarily require a workaround. Known issues are typically documented in section 7 of the Readme file. Readme files for Trend Micro products, along with the latest copies of the product manuals, can also be found in the Trend Micro Download Center:

http://www.trendmicro.com/download/

Known issues can be found in the technical support Knowledge Base:

http://esupport.trendmicro.com

Trend Micro recommends that you always check the Readme file for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

TrendLabs

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery.

Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Appendix B

High Availability, LAN Bypass, and Frequently Asked Questions (FAQs)

This appendix describes how the LAN bypass feature can function under some error conditions and to use two Deep Edge devices in a High Availability environment.

Topics include:

About LAN Bypass

The LAN bypass function allows the network traffic to be bypassed under specific error conditions.

Note

Deep Edge only supports LAN bypass functionality in Bridge Mode.

Use one of the following setting to configure the LAN bypass functions:

- **Auto-Bypass:** For this option, the LAN bypass function is off when the system is in a normal state; the LAN bypass mode is ON when system detects an abnormal state such as kernel panic issue or when power is cut off from the Deep Edge unit
- **On**: Always bypasses traffic
- **Off**: Never bypasses traffic

Note

When the LAN-bypass function is set to ON, the data interface is not available. However, the customer can still access Deep Edge via the separate management interface, if configured.

The LAN-bypass function supports two port Silicom cards:

- **SD:** PXG2BPFIL-SD, PXG2BPI-SD
- **Non-SD:** PEG2BPFID, PEG2BPI

Configuring LAN Bypass

The following procedure allows you to change the default settings for the LAN bypass feature. Change the parameters when you are:

- Installing a new LAN bypass card
- Selecting NICs supporting LAN bypass for the bridge configuration

- Changing the default LAN bypass mode

If you configure the bridge with NICs from the LAN bypass card, it is enabled with the default AUTO setting. Under the AUTO setting, Deep Edge monitors critical services and OS kernel for crashes. If it detects an unrecoverable error, it will open the NIC into "fail open" or bypass mode.

Use the **`show bridge lanbypass mode`** command to check LAN bypass status on Deep Edge.

To display, enable/disable, or change the LAN-bypass service on the Deep Edge unit:

Procedure

1. Log on the CLI interface.
2. Execute the commands in the following table as necessary:

COMMAND	DESCRIPTION
`Enable`	Enters privileged mode so privileged commands can be provided.
`show bridge lanbypass mode`	Displays the current configuration status of the LAN-bypass function.
`configure bridge lanbypass on`	Always bypasses traffic. After running this command, all traffic will be bypassed by LAN bypass card. You will not be able to access the Deep Edge device from the network data interface.
`configure bridge lanbypass off`	Never bypasses traffic. The system will not adjust the LAN bypass status at any time.
`configure bridge lanbypass auto`	The system auto-adjusts the LAN bypass status. For example, when system starts and stops, the bypass function turns off and turns on. When system is in an abnormal state (such as kernel panic), the bypass turns on. After recovery, the bypass turns off automatically.

High Availability Overview

One of the most important aspects of security gateways and networks is keeping network traffic flowing. Deploying Deep Edge in a High Availability (HA) configuration significantly reduces potential traffic interruption. This ensures that online systems and critical business processes are not interrupted when the network experiences failures or downtime.

All traffic passes through the security gateway making it a critical component. A network configuration with a single, standalone network security gateway creates a single point of failure that is vulnerable to any kind of hardware, software, or system failure that could interrupt traffic flow. This could compromise the device and bring all traffic on the network to a halt.

The most effective way to eliminate a potential failure from halting network traffic is to configure the device in a HA configuration. High Availability is achieved by configuring Deep Edge devices in a redundant configuration. With redundant Deep Edge devices, if one device fails, network traffic can be routed through the redundant gateway to keep traffic flowing.

Deep Edge provides a strong and flexible, multi-device high availability solution required for many mission-critical firewall and UTM applications.

Deploying Deep Edge in an HA Environment

HA in Bridge Mode

When deploying Deep Edge in Bridge mode, it can provide a high availability environment. *Figure B-1: HA Environment in Bridge Mode on page B-5* shows a typical HA setup for Deep Edge devices in Bridge mode.

In this deployment mode, the external routers must be able to use either the Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP). For the best configuration method, see the switch or router documentation.

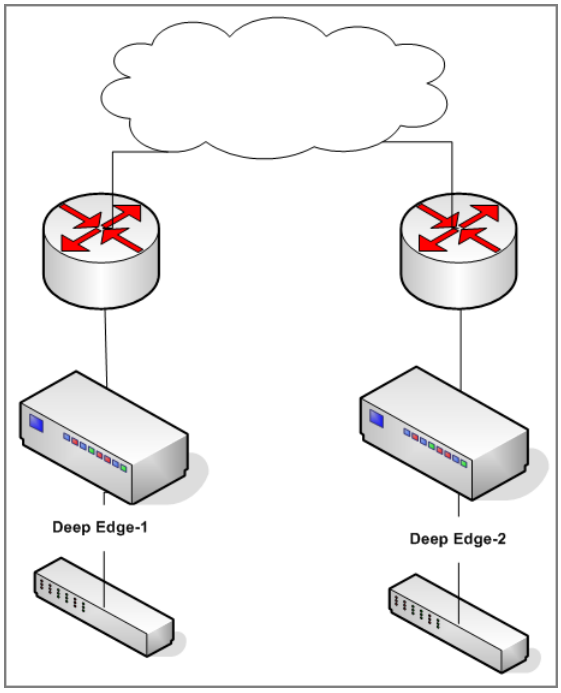


FIGURE B-1. HA Environment in Bridge Mode

High Availability Using OSPF Protocol

Deep Edge can be deployed in High Availability mode using the Open Shortest Path First (OSPF) protocol. See *Figure B-2: HA Deployment using OSPF on page B-6* for an example of Deep Edge in a HA network deployment using OSPF. More information

about OSPF is available in the *Processing and Identifying Traffic* chapter of the *Deep Edge Administrator's Guide*.

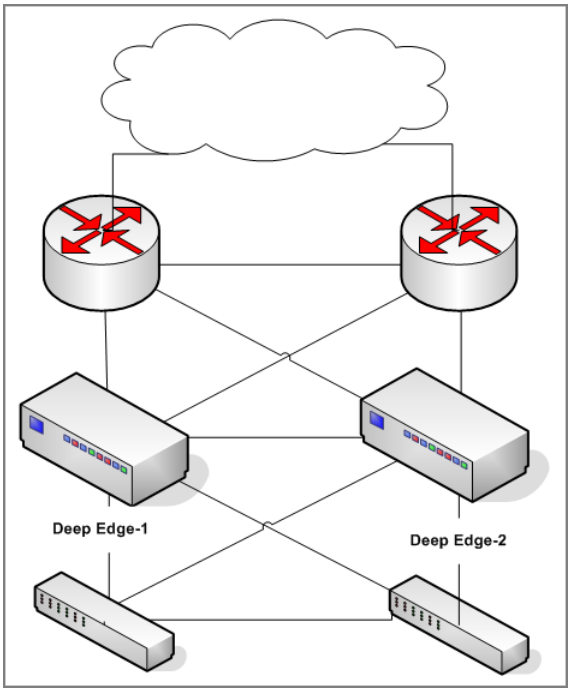


FIGURE B-2. HA Deployment using OSPF

FAQs

Frequently asked questions are a quick way to find solutions. For details about other available support options, see *Troubleshooting Resources on page A-2*.

What happens when Deep Edge hardware fails?

For hard disk failure, no action is taken. For power failure, the LAN-bypass option can be used if previously configured. See *Configuring LAN Bypass on page B-2*.

How do you re-route traffic to a second Deep Edge if the first one fails?

Configure using the Open Shortest Path First (OSPF) protocol. See the *Figure B-2: HA Deployment using OSPF on page B-6* for an example of Deep Edge in a HA network deployment using OSPF.

More information about OSPF is available in the *Processing and Identifying Traffic* chapter of the *Deep Edge Administrator's Guide*.

How do you re-route traffic from Deep Edge if the primary downstream device (switch or router) fails?

Configure the Deep Edge device using the OSPF protocol as shown in *Figure B-2: HA Deployment using OSPF on page B-6*.

What happens when a device that supports Deep Edge—but does not directly process traffic—fails?

It depends on the device:

- Directory server: Already supports failover
- DNS server: Already supports failover
- Trend Micro ActiveUpdate server: Wait for the next scheduled update or manually update.

How do I know if LAN bypass has been activated?

When the LAN bypass is on, the Deep Edge web console is still available. The bandwidth status and session information will both be empty.

Appendix C

Applying Software Patches

This appendix describes how to download and apply software patches for Deep Edge.

Topics include:

Overview

Trend Micro provides the latest product patches that are applicable to the Deep Edge product you installed. These critical patches are version specific and are available for download from the Trend Micro Download Center.

The following sections describe the procedures for downloading new patches, backing up the current configuration (optional), and applying the software patch to Deep Edge.

Backing Up the Current Configuration

Deep Edge configuration back ups can be restored after a patch has been applied.

Procedure

1. At the web console, go to **Administration** > **Maintenance** > **Backup/Restore**.
2. Under **Backup Configuration**, click **Create a Backup**.

   The backup file downloads.

The current Deep Edge configuration is now saved.

Applying a Software Patch

After downloading the product patch and optionally backing up the current configuration, apply the update to Deep Edge.

The manual update feature is also useful when a pattern file is corrupted and must be downloaded again from the update server.

Procedure

1. Download the patch.

   Contact Trend Micro Technical Support for information about available patches.
2. At the web console, go to **Administration** > **Updates** > **Software Patches**.

3. Under **Select a Patch to Install**, click **Browse**.

   A **Open** dialog box appears.

4. Navigate to the folder with the downloaded file, select the file, and then click **Open**.

5. Click **Upload**.

   You are ready to restore the configuration that was previously saved or begin a new configuration.

What to do next

Follow the patch on-screen instructions to apply the patch.

Restoring the Previous Configuration

A previous Deep Edge configuration can be restored after a system failure or upgrade.

Procedure

1. At the web console, go to **Administration** > **Maintenance** > **Backup/Restore**.

2. In the **Restore Configuration** section, click **Browse**.

   A **Open** dialog box appears.

3. Navigate to the folder with the stored the backup file, select the file, and then click **Open**.

4. Click **Restore**.

The Deep Edge configuration backup is restored. You are now ready to make further configuration changes or begin using Deep Edge.

Appendix D

Testing and Configuring Deep Edge

After opening the Deep Edge web console, there are several procedures that help to test and verify that Deep Edge is working properly.

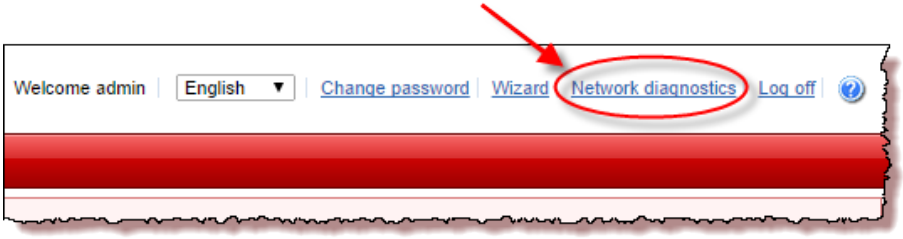
Topics include:

Network Diagnostics

The Network Diagnostics tool helps troubleshoot common connectivity issues, including:

- Internet access
- DNS configuration
- Traffic routing
- Trend Micro ActiveUpdate access
- Trend Micro Web Reputation Service (WRS) access

Access the Network Diagnostics tool by clicking **Network Diagnostics** from the web console's top menu.



Testing the Passage of HTTP Traffic

Use this test to verify that the network settings are correct and that normal HTTP traffic can pass through Deep Edge. Deep Edge must already be deployed in Route or Bridge mode. See the *Deep Edge Deployment Guide* for details.

Procedure

1. Log on an internal endpoint.
2. Access the sample URL: http://www.trendmicro.com

If Trend Micro's homepage displays correctly, Deep Edge is deployed correctly.

3. Access an internal URL, if you deployed Deep Edge only for internal use only .

   If the internal URL you accessed appears, Deep Edge is deployed correctly.

EICAR Test File

The European Institute for Computer Antivirus Research (EICAR) has developed a test virus to test your antivirus protection. This script is an inert text file. The binary pattern is included in the virus pattern file from most antivirus vendors. The test virus is not a virus and does not contain any program code.

WARNING!

Never use real viruses to test Internet security.

Download the EICAR test virus from the following URL:http://www.eicar.org/download/eicar.com.txt

Alternatively, create an EICAR test virus by typing or copying the following into a text file, and then naming the file `eicar.com`:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
$H+H*
```

Note

Flush the local browser cache before testing. If the local browser cache contains a copy of the test virus, it is possible an attempt to download the file would get the file from the cache, rather than getting it from the Internet, and Deep Edge would not detect the file.

Testing with the EICAR Test File

Procedure

1. Log on to the Deep Edge web console.
2. Click **Policies** > **Rules**.
3. Click the default policy to edit it.
4. Click the **Schedule and Action Profile** tab.
5. Set the schedule to **Always** action
6. Set the action profile to **General Scan**.
7. Click **OK**.
8. For the same policy, click the **Traffic Type** tab.
9. Click the top **Selected** radio button to display the **Application Group** and **URL Category Group** options.
10. Configure a default URL category rule.
    a. Expand the **Default URL Categories**.
    b. Select the **Adult** check box.
    c. Click **OK**.
11. Click **Apply** at the top of the **Rules** page.
12. Use a test client to access the following website and download a test virus:

    http://www.eicar.org/download/eicar.com.txt
13. Use a test client machine to access the following website twice:

    http://wrs21.winshipway.com
14. Use a test client machine to access the following website twice.

    http://wrs61.winshipway.com/

15. Wait 30 seconds and then go to **Analysis & Reports** > **Log Analysis** > **Internet Security**.
16. Perform an Information Security logs query for information about violation.

Testing Web Reputation

Procedure

1. Open a web browser and specify the following text in the address field:

   `http://wrs21.winshipway.com`

2. Flush the local browser cache and access the same URL again.

   If the test is successful, you should receive a Deep Edge Security Event message stating:

   Access to this web site was blocked by an IT policy because of its web reputation score.

Testing Application Control

Use the following procedure to modify the Deep Edge Security Policy to block end-users from accessing the Google website.

Procedure

1. Log on the Deep Edge web console.
2. Click **Policies** > **Rules**.
3. Click the default policy to edit it.
4. Set the tabs as follows:

OPTION	DESCRIPTION
Sources and Users	For **Source Addresses**, select **Any**. For **Users and Groups**, select **Any**.
Destinations	For **Destination Address**, select **Any**.
Traffic Type	Select the **Selected** check box, expand **Default Applications** > **Web** and then select the **Google** check box.
Schedule and Action Profile	For **Schedule**, select **Always**. For **Action**, select **Block**.

5. Click **OK**.
6. Click **Apply** at the top of the **Rules** page.
7. Open a web browser and attempt to access http://www.google.com.

   If the test is successful, the browser will not display the Google website.

Testing URL Filtering

Trend Micro recommends using the default settings to test URL filtering.

Procedure

1. Log on the Deep Edge web console.
2. Click **Policies** > **Rules**.
3. Click the default policy to edit it.
4. Set the tabs as follows:

OPTION	DESCRIPTION
Sources and Users	For **Source Addresses**, select **Any**. For **Users and Groups**, select **Any**.
Destinations	For **Destination Address**, select **Any**.
Traffic Type	Select the **Selected** check box, expand **Default URL Categories** and then select the **Communications and Search** check box.
Schedule and Action Profile	For **Schedule**, select **Always**. For **Action**, select **Block**.

5. Click **OK**.
6. Click **Apply** at the top of the **Rules** page.
7. Open the browser and attempt to access http://www.google.com.
8. Flush the browser URL cache and attempt to access http://www.google.com again.

   If the test is successful, the browser displays a Security Event notification. It does not display the Google website.

Index

W

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: CTEM26693/140930