

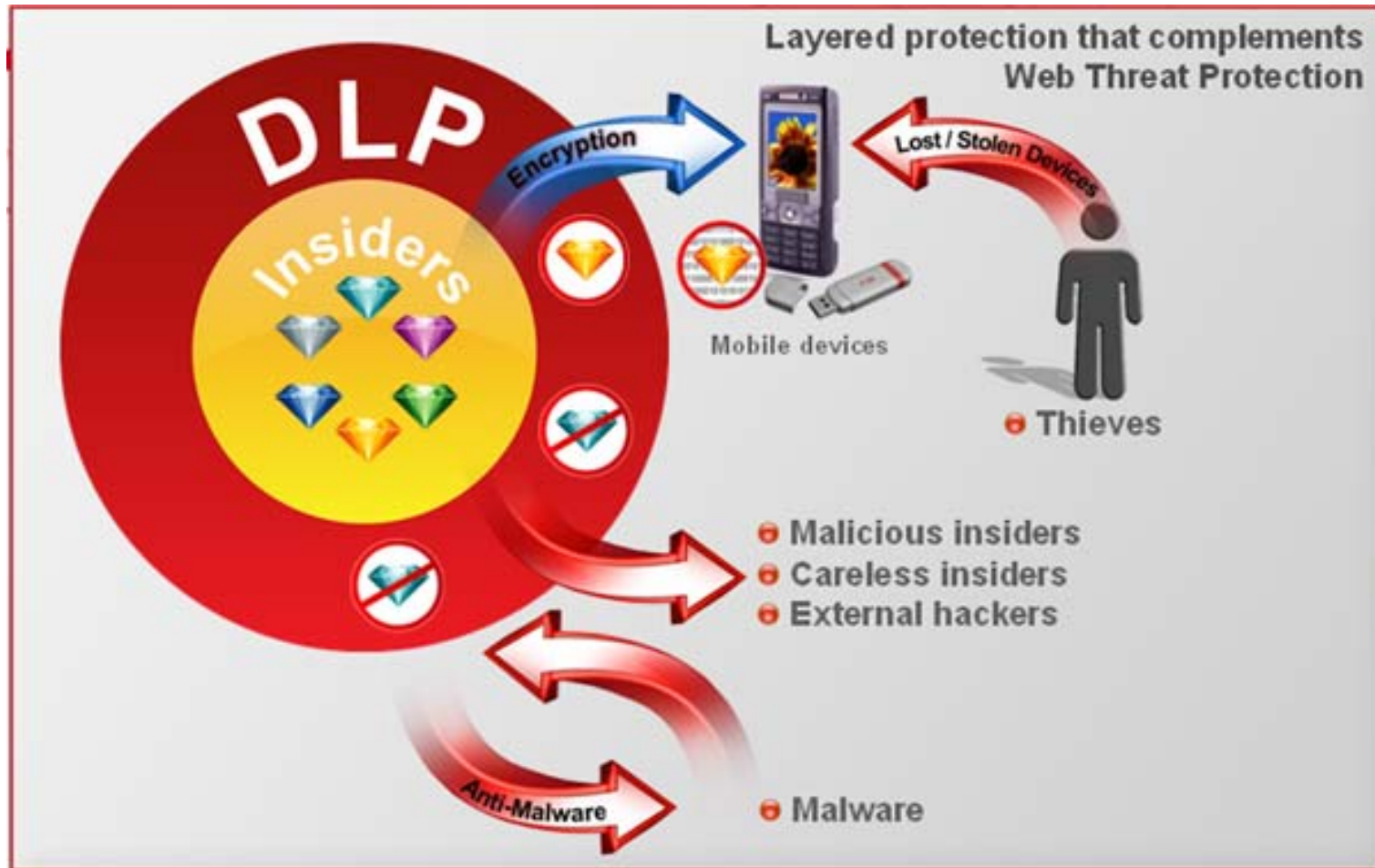
DLP Network Monitor 2.0 Training

趋势科技技术支持部
Mac Tang

Agenda

- ▶ *DLP5.5*介绍
 - ◆ *DLP5.5*系列的产品体系结构和机制
 - ◆ *DLP5.5*系列的各个组件
 - ◆ *DLP5.5*新功能
- ▶ *NDLP2.0*介绍
 - ◆ 什么是*NDLP*?
 - ◆ *NDLP*的产品优势?
 - ◆ *NDLP*如何部署?
 - ◆ *NDLP*的系统需求和安装步骤
 - ◆ *NDLP*安装后的验证和使用
 - ◆ *NDLP*的常见问题和解决

DLP5.5介绍



DLP5.5介绍

▶ *Data Loss Prevention* → 简称 *DLP*

- ▶ 数据丢失预防 (*DLP*) 是防止意外和恶意数据泄漏的关键所在---不论是客户信息, 财务数据, 知识产权还是商业机密。一次事故可能导致品牌声誉受损、丢失业务、罚款或法律诉讼从而造成数百万元的损失。
- ▶ 数据丢失面临的难题就是如何识别, 跟踪并保护所处于闲置、使用和移动状态的机密数据。这项工作正在因为风险因素的增加而变得日益困难, 包括陷入失业恐慌的失业员工, 移动工作人员以及**3G** 网卡, **WIFI**设备, **USB**驱动器, 网络电子邮件, 即时通讯和**CD/DVD**之类的泄漏渠道。
- ▶ 趋势科技 *Data Loss Prevention* 是一种数据丢失预防 (*DLP*) 解决方案, 凭借最广泛的覆盖范围, 最出色的性能和灵活部署, 而降低了其复杂性和成本。

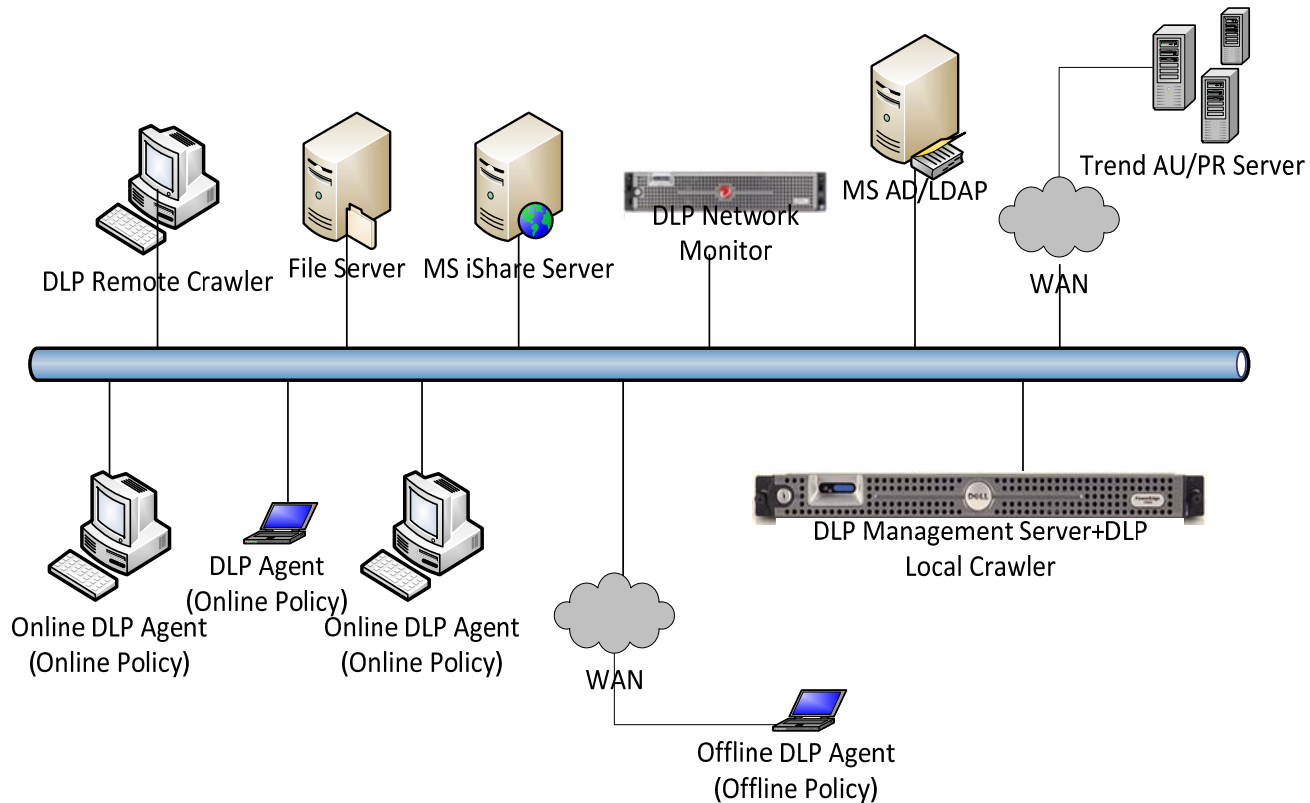
DLP5.5介绍

▶ DLP的主要益处

- ▶ 保护隐私，知识产权保护---发现、监测并预防机密数据/敏感数据丢失，识别，检测并保护商业机密，不论是在线还是离线。
- ▶ 教育和补救---可以定制警告弹出框，允许员工提出申辩理由，阻止和警告危险的员工行为和数据丢失。
- ▶ 发现敏感数据---通过扫描，可以发现员工的笔记本、桌面电脑和服务器中心上存在的已知敏感数据。
- ▶ 威胁保护---外部保护：数据窃取软件、黑客。内部保护：意外数据丢失，恶意数据丢失。

DLP5.5介绍

▶ DLP系列的产品体系结构和机制



DLP5.5介绍

▶ DLP系列的产品体系结构和机制

| | |
|--|--|
| Fingerprint Matching (指纹匹配) | 指纹匹配能够对非结构化的内容文档进行最佳操作，DLP提取并存储敏感文档后，如果终端用户尝试传输一个文件，DLP会提取传输的文件指纹信息与已保存的指纹库进行匹配。如果两者具有相同点，DLP将计算两者之间的相同点的比例。DLP设定匹配等级分为高、中、低，相同越高匹配等级越高，一旦匹配等级达到DLP设定的等级，DLP则把此文件视为敏感文件。DLP存储的指纹大小取决于文件的数量和大小。 |
| Pattern Matching (模板匹配) | DLP基于用户自定义的样式进行匹配，例如身份证号等，DLP能够与非结构化的内容文档进行最佳操作，例如信用卡号、身份证信息、电话号码等。管理员可以通过正则表达式自定义Pattern |
| Keyword Matching (关键字匹配) | DLP可以根据关键字进行匹配 |
| File Attribute Matching (真实文件类型匹配) | DLP可以根据文件的类型进行匹配，特别的是DLP具有真实文件类型的检测能力，即时文件扩展名已经被更改或者无扩展名的文件。 Compliance template匹配 |

DLP5.5系列的各个组件

▶ DLP5.5系列的各个组件

▶ Data Loss Prevention Management Server (服务端)

- ▶ DLP服务端是一款硬件设备，提供集中控制管理、策略配置和下发、产品组件更新、日志查询、报表生成、数据指纹获取等中央控制管理操作平台

▶ Data Loss Prevention Endpoint (客户端)

- ▶ DLP客户端可以检测数字资产并自动根据公司策略设定对泄密的操作做出阻止、日志记录、加密、警告等操作。
- ▶ 支持多种Channel的检测，支持识别并处理300多种文件类型。

▶ Data Loss Prevention Network Monitor 2.0 (网络监控)

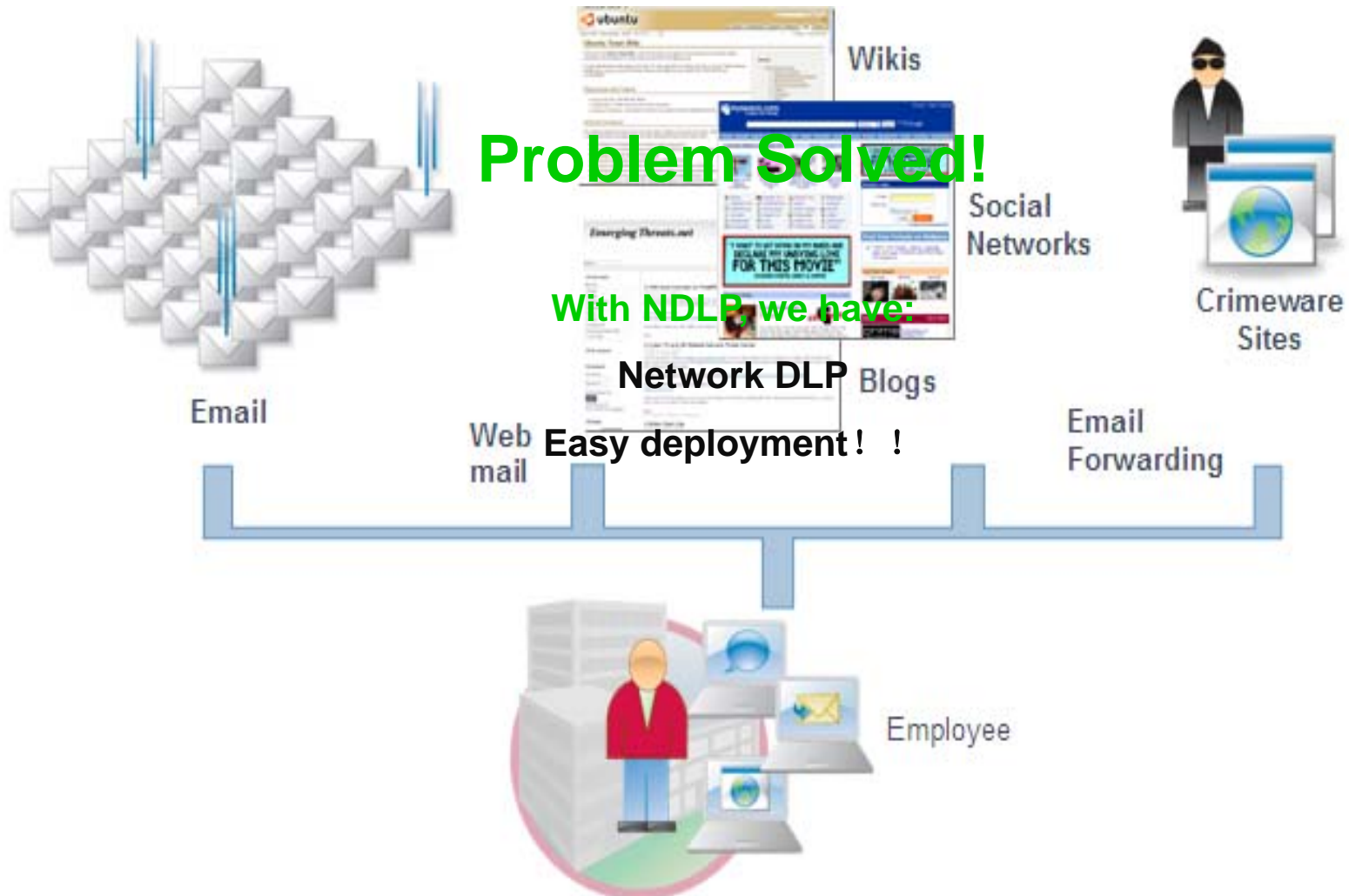
- ▶ TMDLPMN是一款基于扫描网络镜像数据，通过监控网络数据流量来检测数据威胁的产品：
- ▶ 检测内网与外网的敏感信息数据传输，包括：**SMTP, HTTP, FTP, IM (AIM/AOL, MSN, Yahoo Messenger), and Webmail (Hotmail, Gmail, Yahoo)**
- ▶ 支持最常用的局域网文件共享**SMB**协议。

DLP5.5新功能

▶ DLP5.5新功能

- ▶ **Web**控制台界面进一步优化
- ▶ 增加TMDLPMN2.0网络监控产品（需要单独激活）
- ▶ **Remote Crawler**工具：支持**Windows 64**位操作系统
- ▶ 高级日志管理
- ▶ 增加数据防偷窃**Pattern**病毒码组件-- **Network Content Correlation Pattern (NCCP): Data Stealing Malware (DSM)/botnet detection**
- ▶ 基于不同策略设定黑白名单
- ▶ 基于不同策略设定不同弹出警告框内容

NDLP2.0介绍

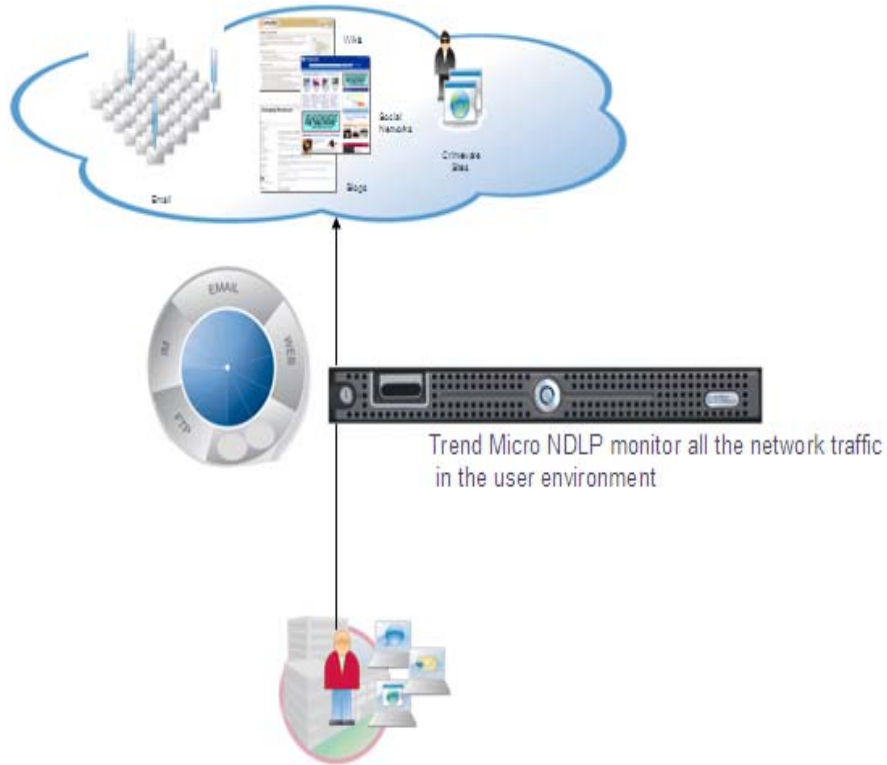


NDLP2.0介绍

▶ 什么是NDLP?

- ▶ **Data Loss Prevention Server (DLP) Network Monitor 2.0**是下一代拥有智能混合计算规则，运算法则，**Pattern**等方式检测敏感数据、文件外泄网络流量检测设备。
- ▶ 以旁路部署模式部署在用户网络，侦听数据镜像口。
- ▶ 支持针对OSI参考模型2-7层的应用进行检测。

Web2.0后越来越多遇到的问题



NDLP2.0介绍

▶ NDLP的产品优势

- ▶ 通过监控网络镜像流量，针对数据包扫描，检测/发现敏感文件，违规的源和目标IP，匹配违反的法规遵从，以及通过Pattern比对来检测恶意的数据偷窃。
- ▶ 与DLP Management Server联动，接收策略和Pattern下发和管理，以及日志整合
- ▶ 部署简单，监听交换机Incoming和Outgoing流量的数据镜像口，无需改变用户网络架构和中断网络
- ▶ 无需在终端PC上安装客户端程序，检测发现敏感文件外泄，利于公司安全审计。

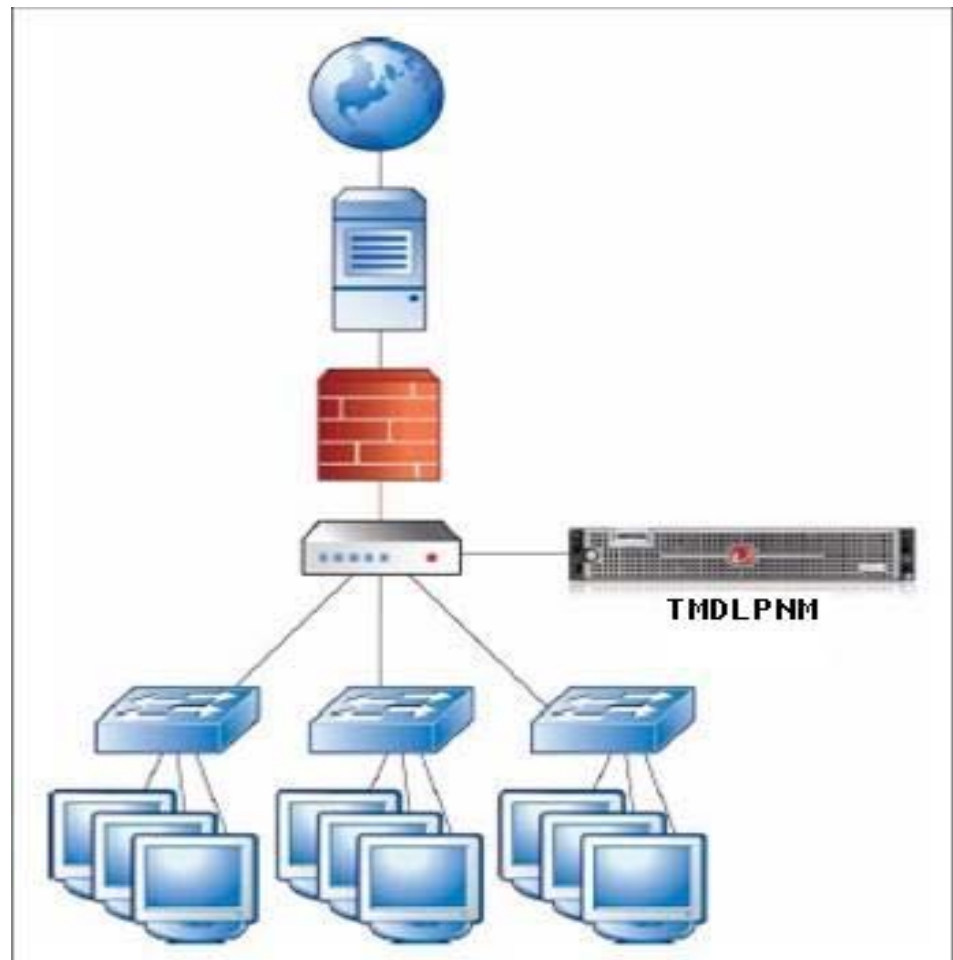
NDLP2.0介绍

▶ NDLP如何部署?

- ▶ NDLP可用光盘安装在DELL R710上,
- ▶ 一个数据口与DLP管理端通信, 剩余端口皆可作为镜像口。
- ▶ 镜像数据**必须**是完整的双向的数据包 (*Incoming+Outgoing*)
- ▶ NDLP最大吞吐率支持**215mbps**流量, **100,000** 并发连接数 (DELL R710标准环境)

NDLP2.0介绍

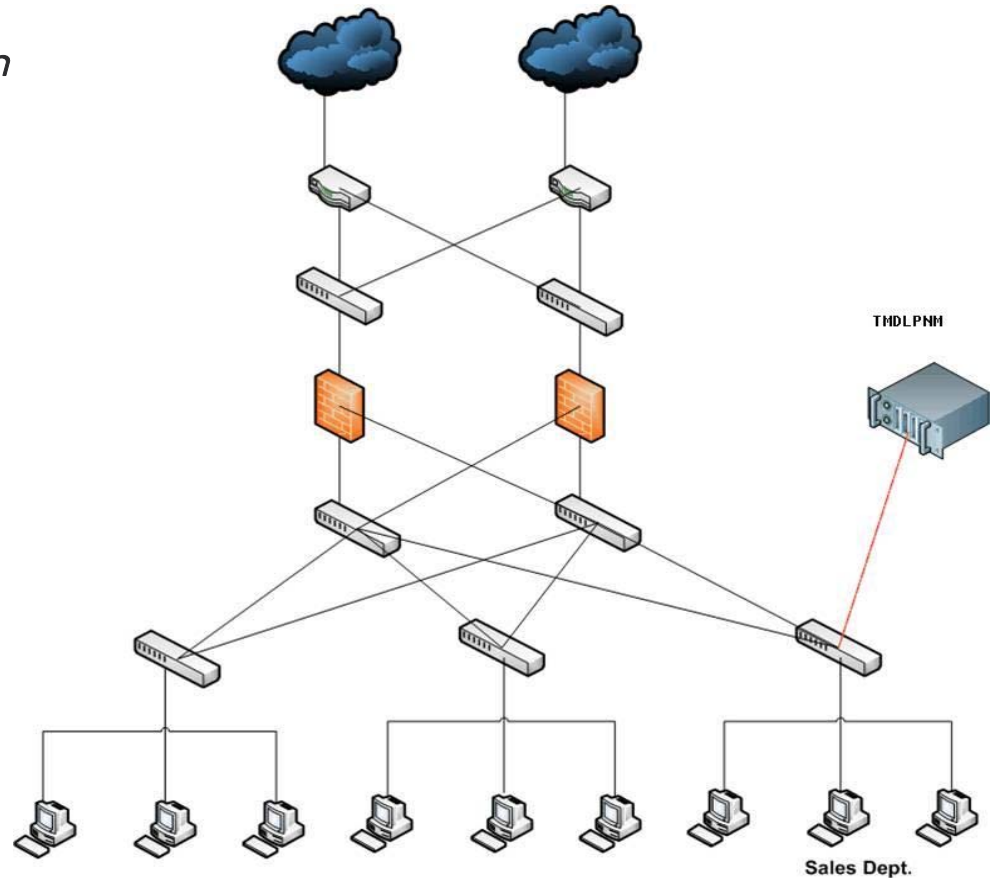
- ▶ *NDLP*如何部署?
 - ▶ 单数据镜像口-----*Core Switch*



NDLP2.0介绍

▶ NDLP如何部署?

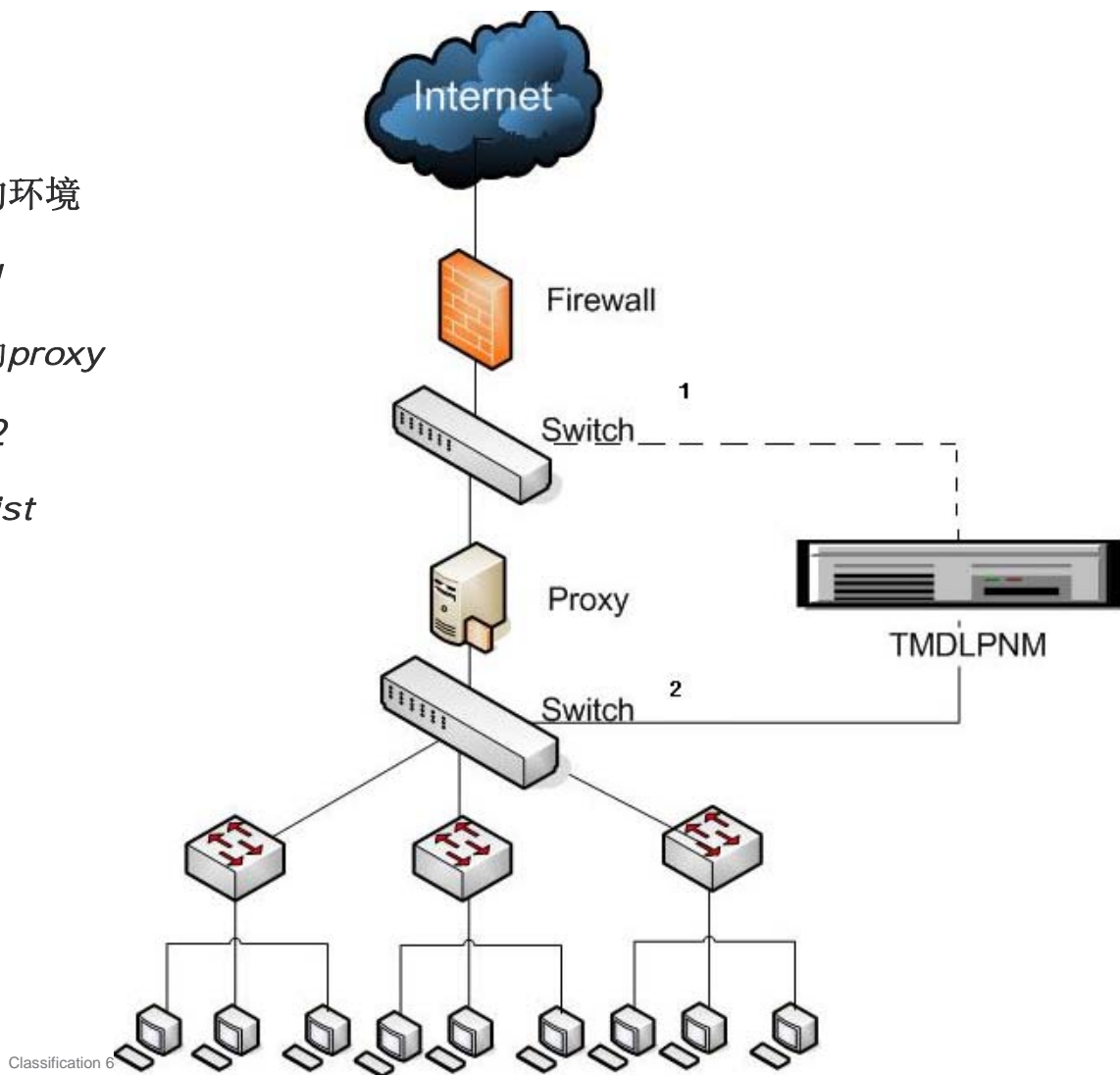
- ▶ 单数据镜像口-----*Distribute Switch*



NDLP2.0介绍

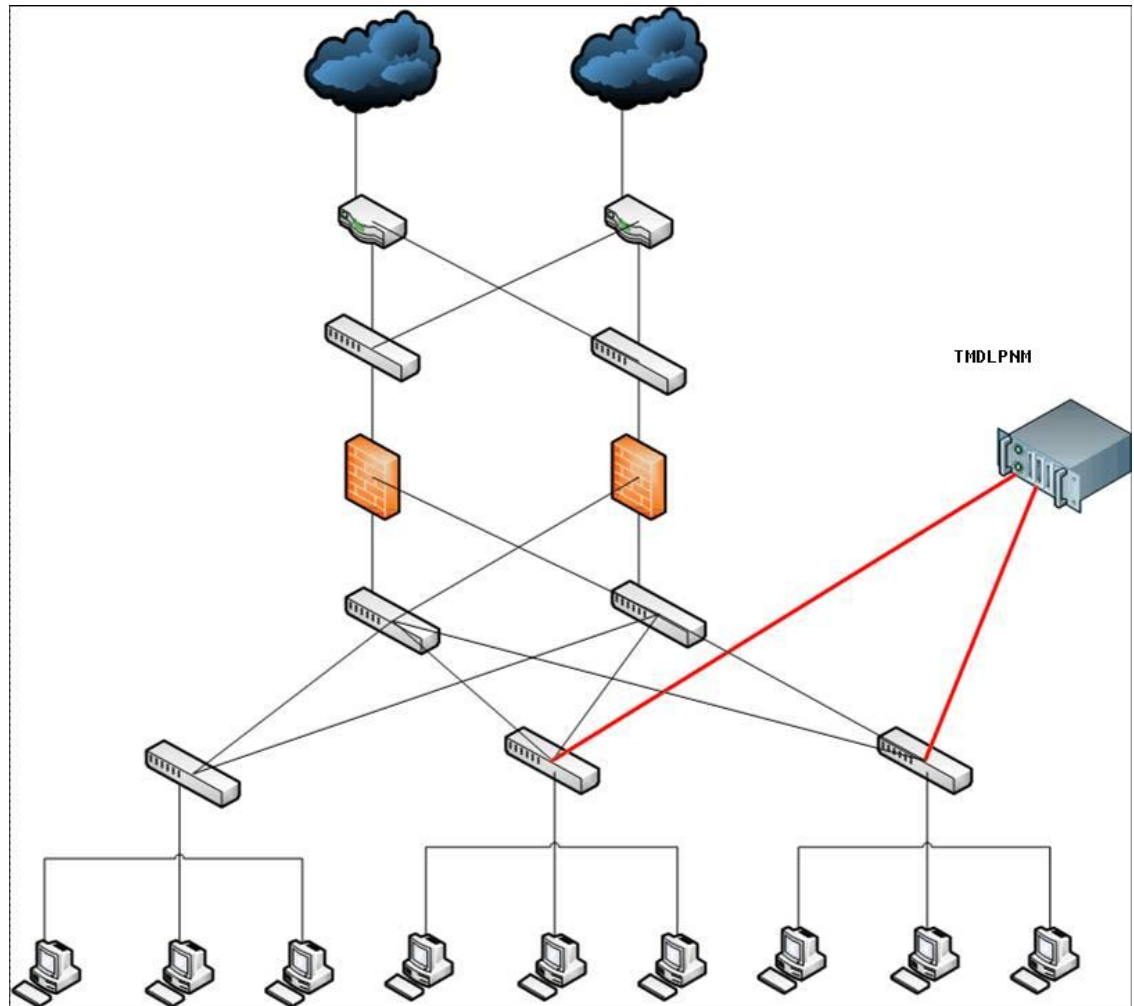
▶ NDLP如何部署?

- ▶ 单数据镜像口 ----存在Proxy的环境
- ▶ 情况1: 如果Mirror口在位置1
 - ▶ NDLP检测到的事件, 源IP为均proxy
- ▶ 情况2: 如果Mirror口在位置2
 - ▶ 将Proxy的IP填入Blocked List



NDLP2.0介绍

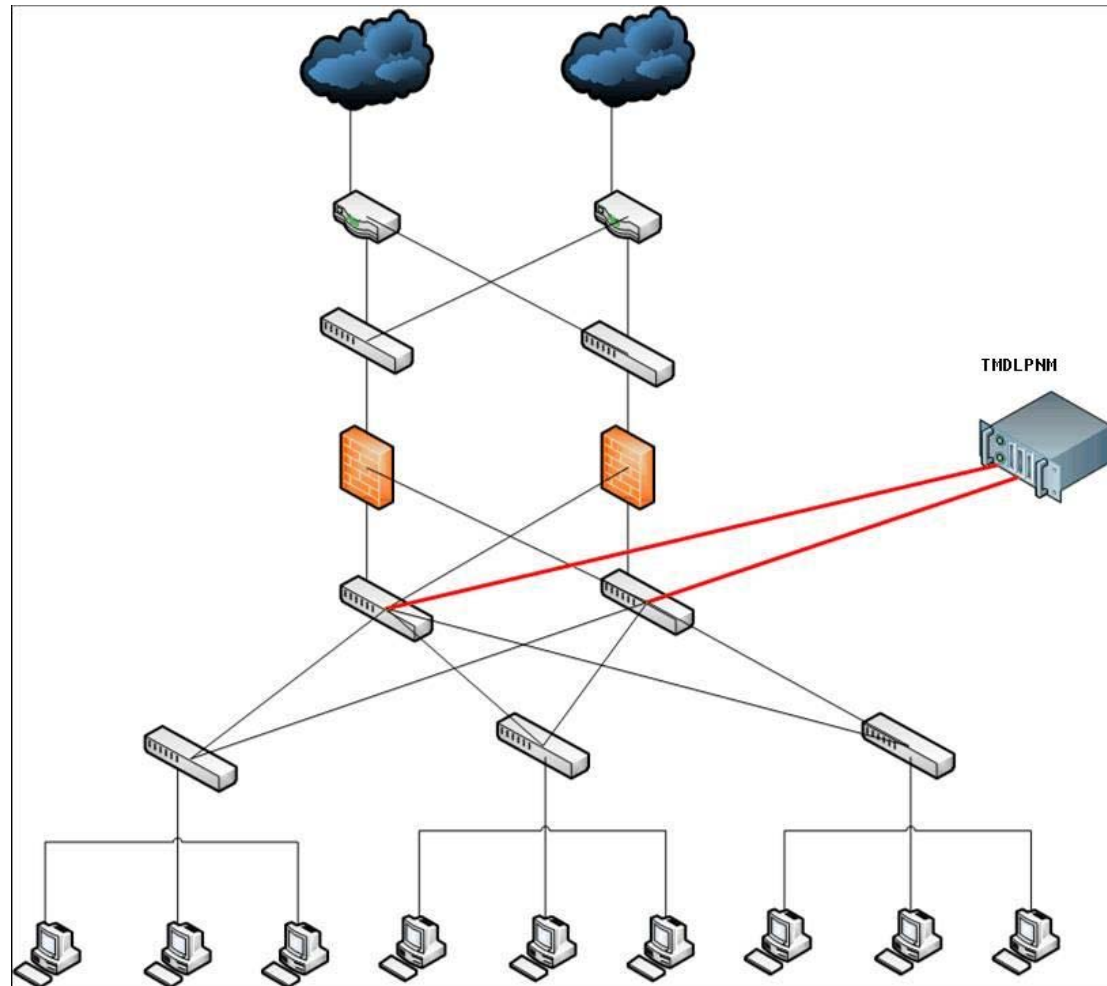
- ▶ *NDLP*如何部署?
 - ▶ 多数据镜像口-----多网段环境



NDLP2.0介绍

▶ NDLP如何部署?

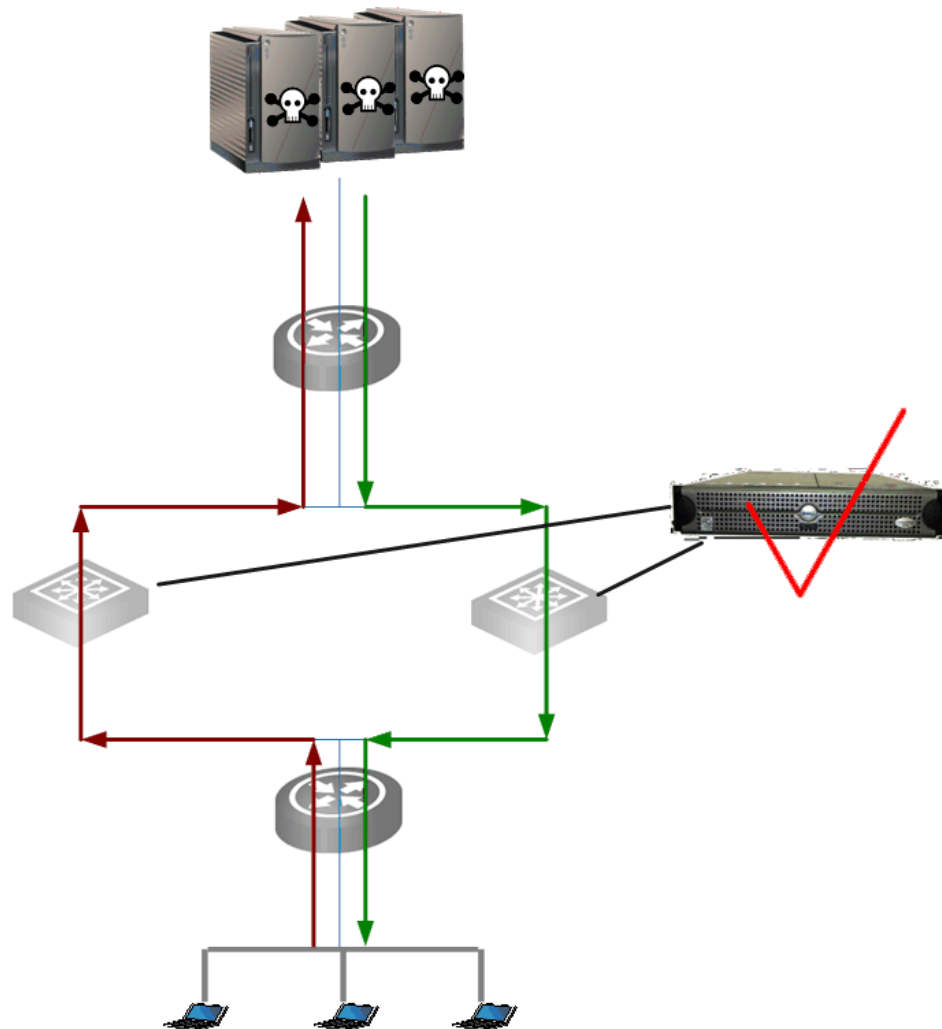
- ▶ 多数据镜像口-----冗余网段环境
- ▶ 主热备环境



NDLP2.0介绍

▶ NDLP如何部署？

- ▶ 多数据镜像口-----非对称路由环境
 - ▶ 必须使得NDLP接收到完整的数据包
 - ▶ 否则将无法检测数据包



NDLP2.0介绍

▶ NDLP的系统需求和安装步骤?

▶ NDLP硬件系统需求

| Unit Owner | NDLP |
|-------------------|--|
| 硬件体积 | Dell R710 2U DxWxH(26.8"x17.44"x3.4") Weight: 26.1Kgs |
| 吞吐量 | 215Mbps |
| 并发连接数 | 100,000 |
| CPU*2 | Intel Quad core E5550 Xeon,2.66Ghz,8M cache |
| 内存 | 8GB (4x2G) 1066MHz |
| 硬盘 | 3.5 SATA (15K RPM): 300GB |
| External NIC card | 2 * Intel® Gigabit ET NIC, Dual Port, Copper, PCIe-4 |
| PSU | 2x 870W |

NDLP2.0介绍

▶ NDLP的系统需求和安装步骤?

▶ NDLP程序安装步骤

▶ 下载地址:

▶ DLP5.5 Server—管理端:

▶ <http://support.trendmicro.com.cn/TM-Product/Product/DLP/5.2/Manager/>

▶ Patch: http://support.trendmicro.com.cn/TM-Product/Product/DLP/5.5/Patch/Patch1_Manager/

▶ NDLP2.0:

▶ http://support.trendmicro.com.cn/TM-Product/Product/TMDLPMN/ISO/2.0_GM/

▶ 文档地址:

▶ DLP5.5 SOP:

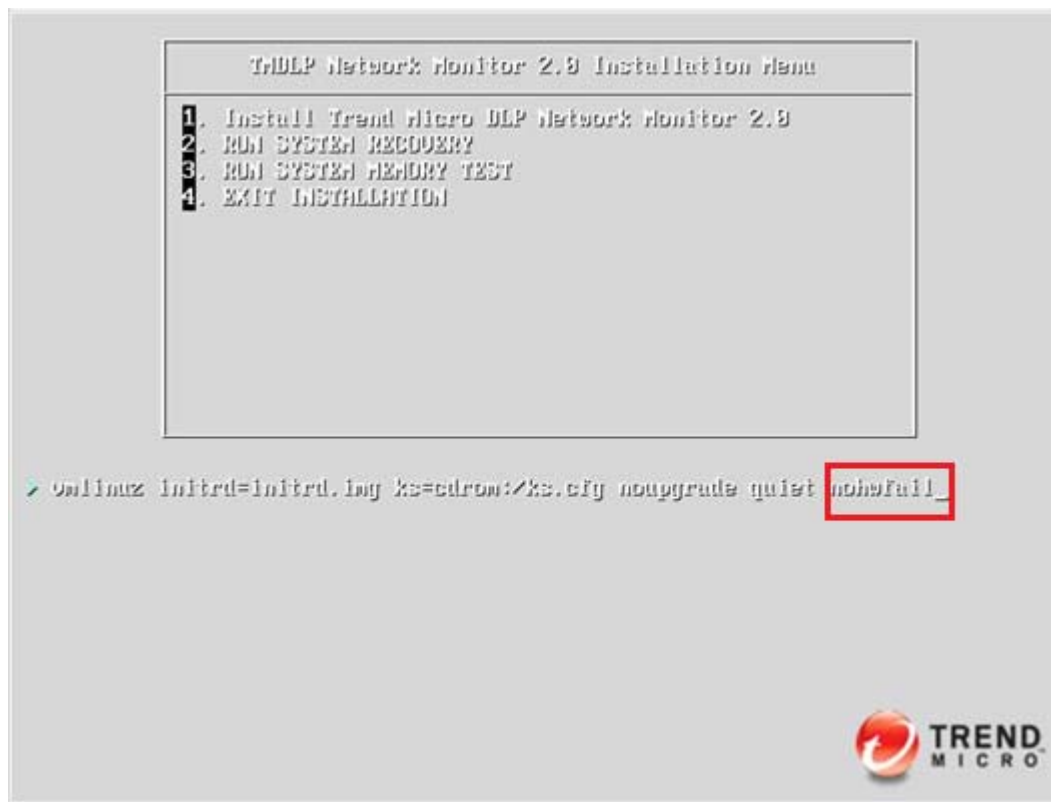
▶ http://support.trendmicro.com.cn/TM-Product/Document/SOP/DLP/Ex_DLP_V5.5_SOP_SC_1.1.pdf

NDLP2.0介绍

▶ NDLP的安装步骤

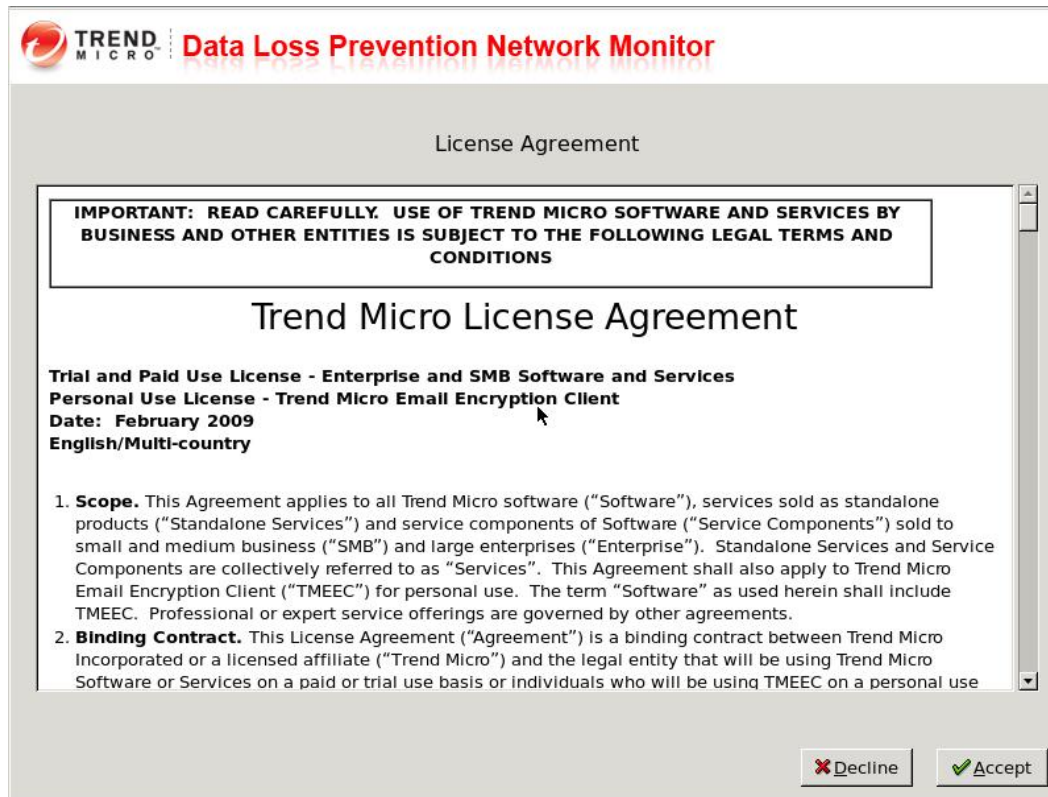
▶ 如果测试环境，配置不符合要求，可以按 **TAB** 键

▶ 输入 *nohowfail*



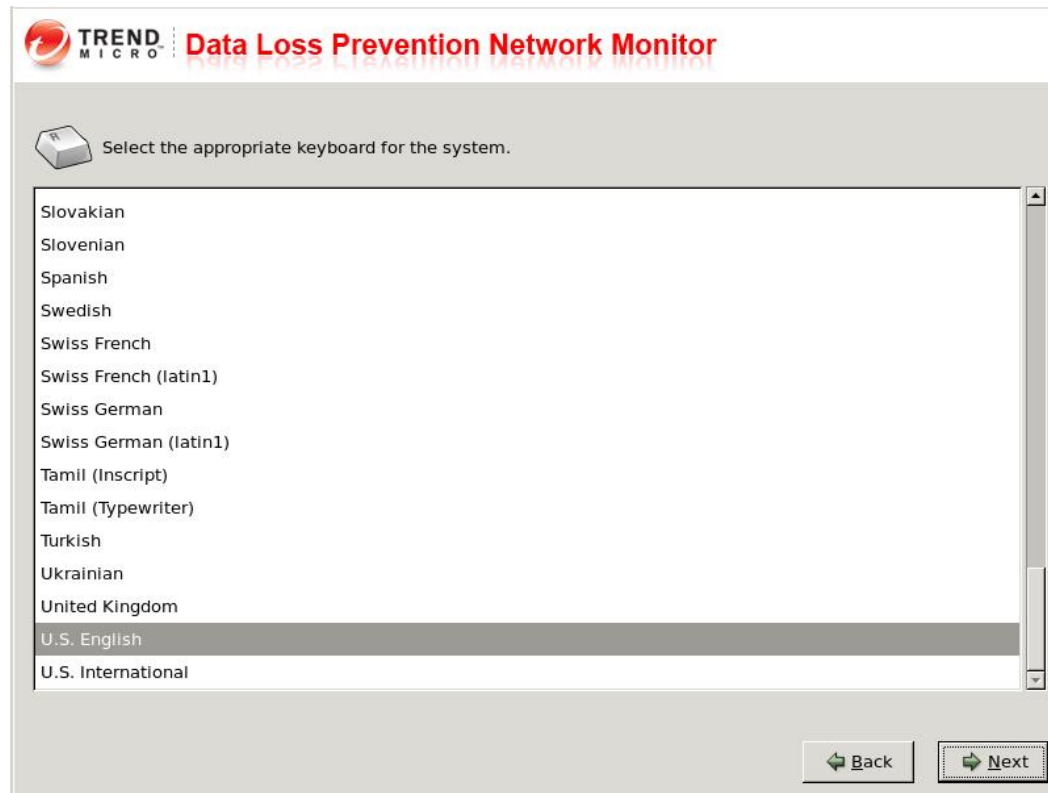
NDLP2.0介绍

▶ NDLP的安装步骤



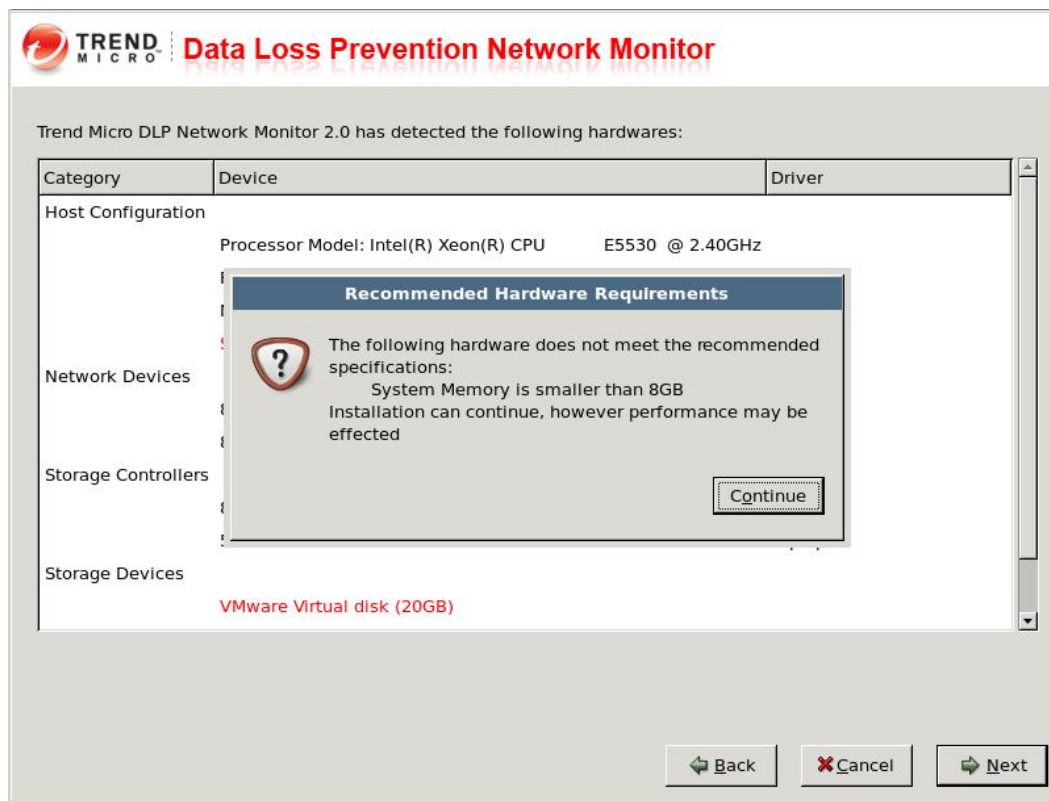
NDLP2.0介绍

▶ NDLP的安装步骤



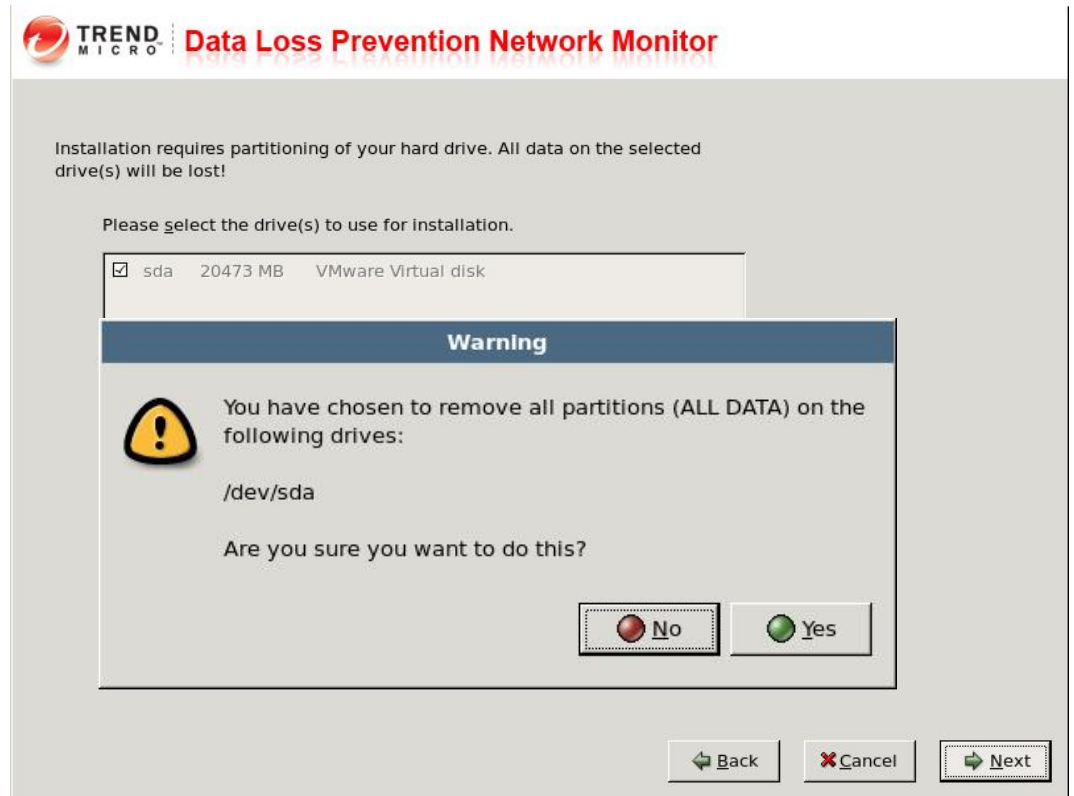
NDLP2.0介绍

▶ NDLP的安装步骤



NDLP2.0介绍

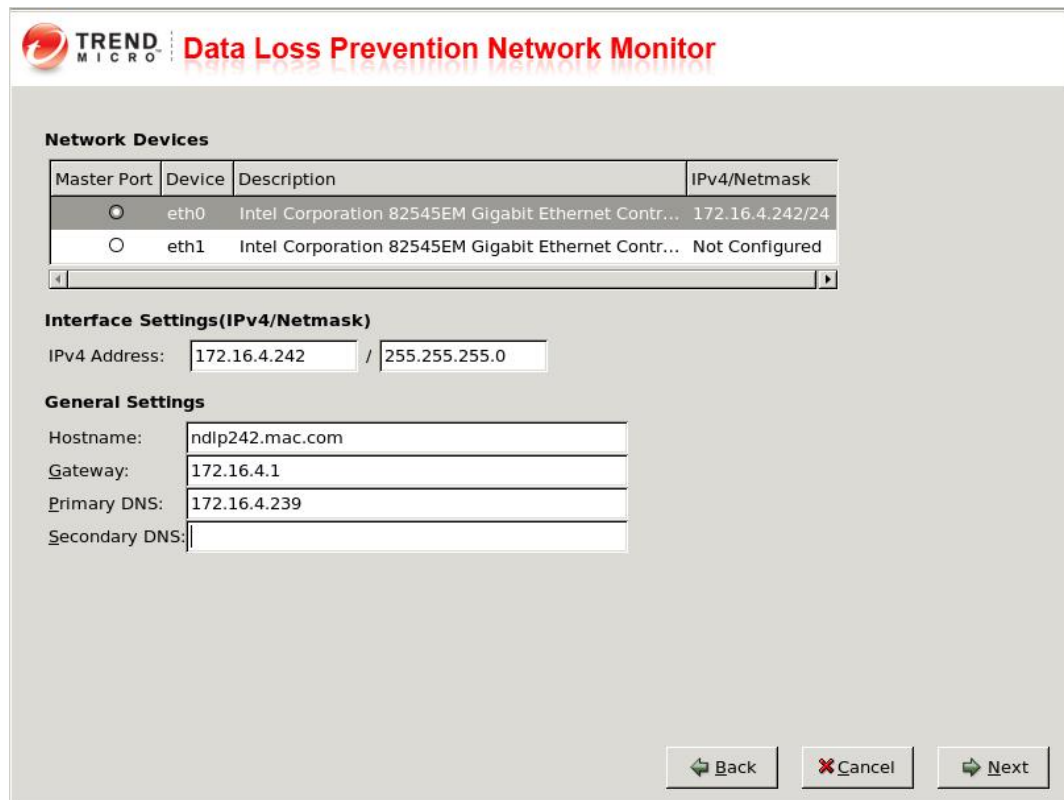
▶ NDLP的安装步骤



NDLP2.0介绍

▶ NDLP的安装步骤

- ▶ *Hostname*需要输入FQDN地址



The screenshot shows the configuration page for the Trend Micro Data Loss Prevention Network Monitor. The interface is titled "TREND MICRO Data Loss Prevention Network Monitor". It contains three main sections: "Network Devices", "Interface Settings (IPv4/Netmask)", and "General Settings".

Network Devices

| Master Port | Device | Description | IPv4/Netmask |
|----------------------------------|--------|---|-----------------|
| <input checked="" type="radio"/> | eth0 | Intel Corporation 82545EM Gigabit Ethernet Contr... | 172.16.4.242/24 |
| <input type="radio"/> | eth1 | Intel Corporation 82545EM Gigabit Ethernet Contr... | Not Configured |

Interface Settings (IPv4/Netmask)

IPv4 Address: /

General Settings

Hostname:

Gateway:

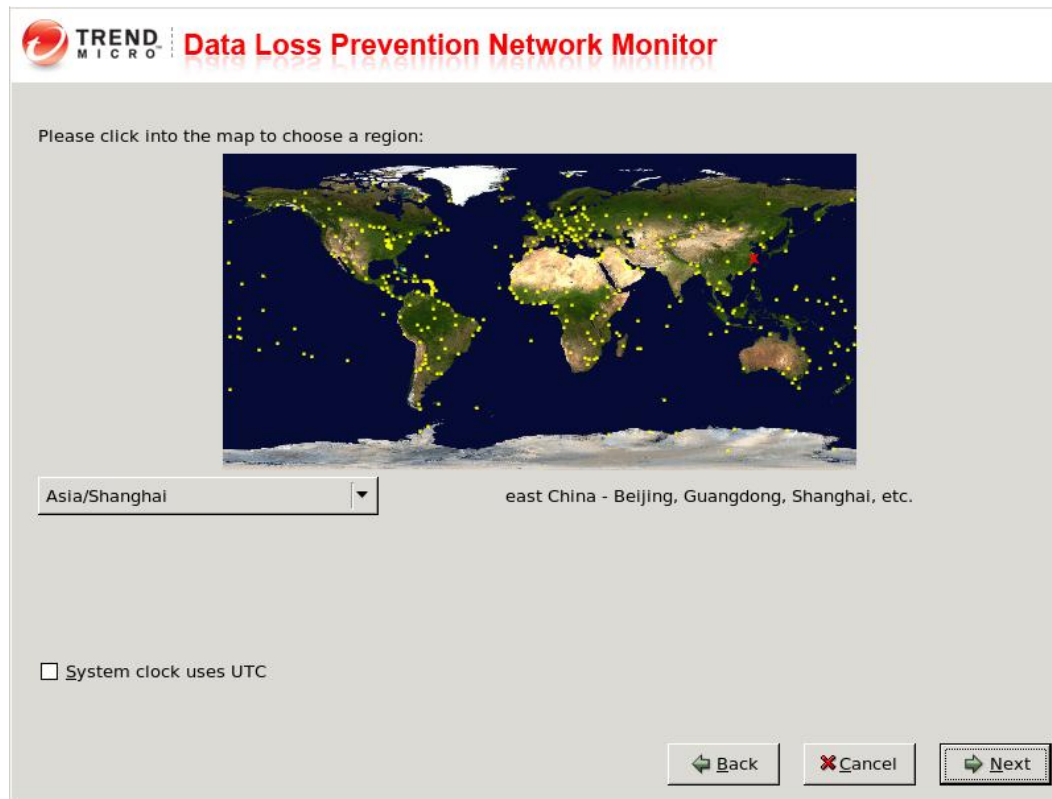
Primary DNS:

Secondary DNS:

At the bottom right, there are three buttons: "Back", "Cancel", and "Next".

NDLP2.0介绍

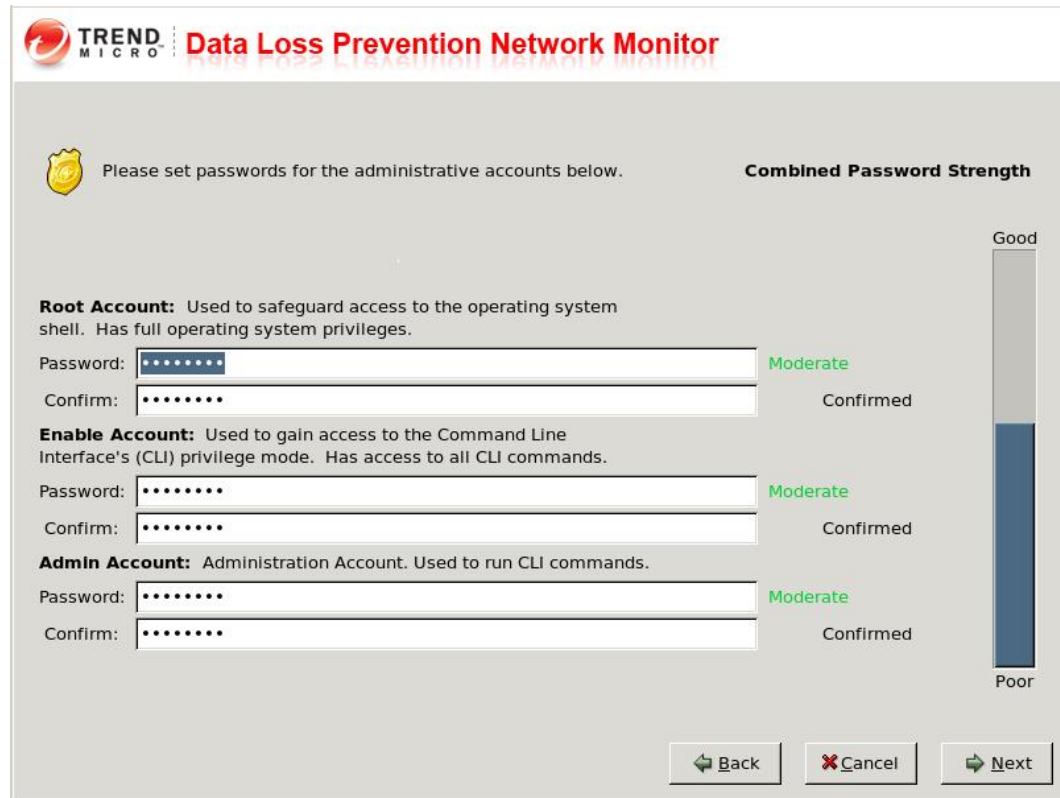
▶ NDLP的安装步骤



NDLP2.0介绍

▶ NDLP的安装步骤

- ▶ 密码最短需要8位



TREND MICRO Data Loss Prevention Network Monitor

Please set passwords for the administrative accounts below.

Combined Password Strength

Good

Poor

Root Account: Used to safeguard access to the operating system shell. Has full operating system privileges.

Password: [Moderate] Confirmed

Confirm: [Confirmed]

Enable Account: Used to gain access to the Command Line Interface's (CLI) privilege mode. Has access to all CLI commands.

Password: [Moderate] Confirmed

Confirm: [Confirmed]

Admin Account: Administration Account. Used to run CLI commands.

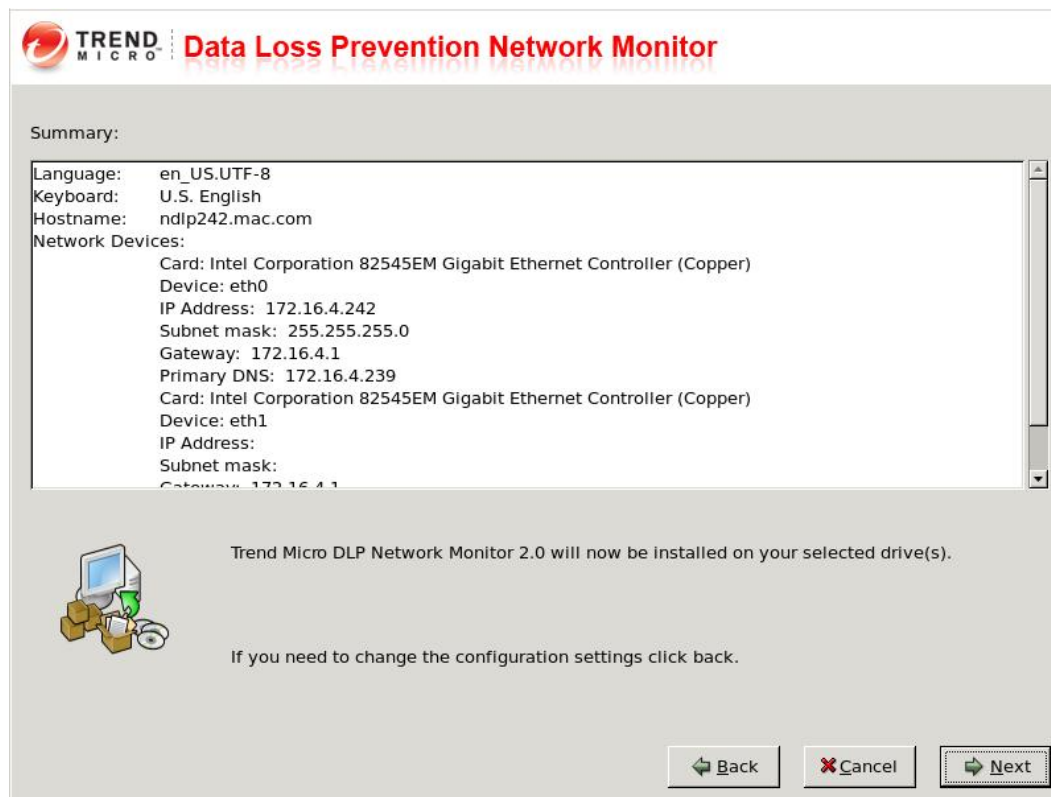
Password: [Moderate] Confirmed

Confirm: [Confirmed]

Back Cancel Next

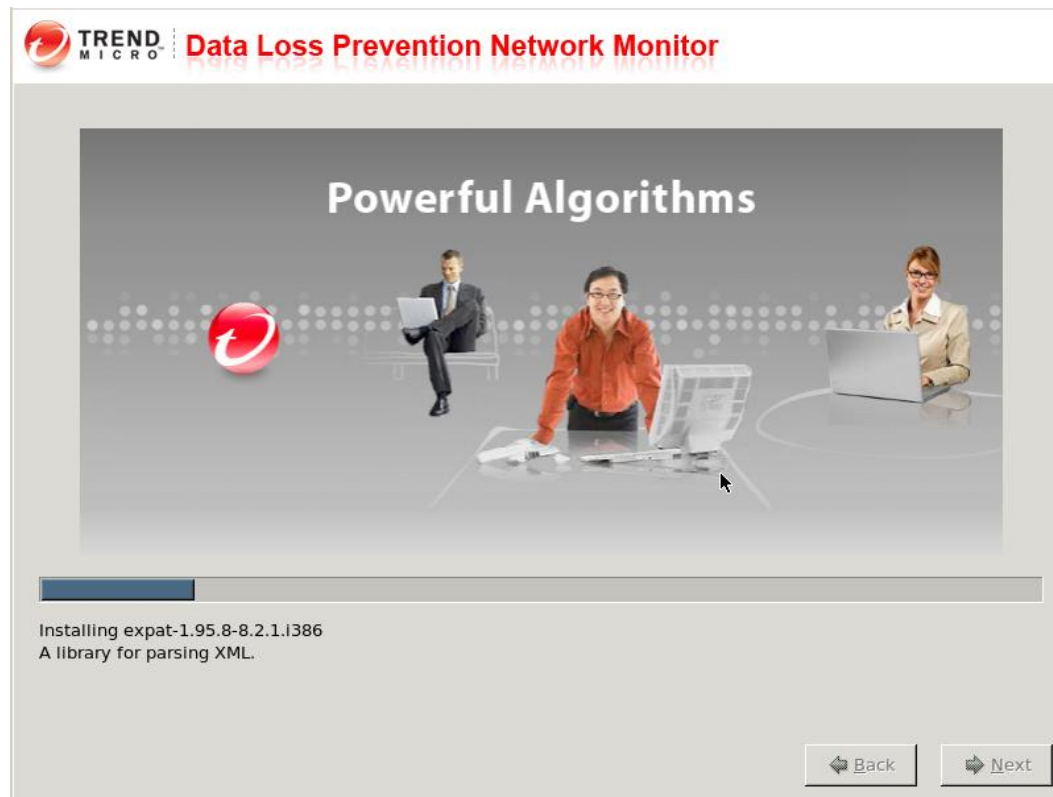
NDLP2.0介绍

▶ NDLP的安装步骤



NDLP2.0介绍

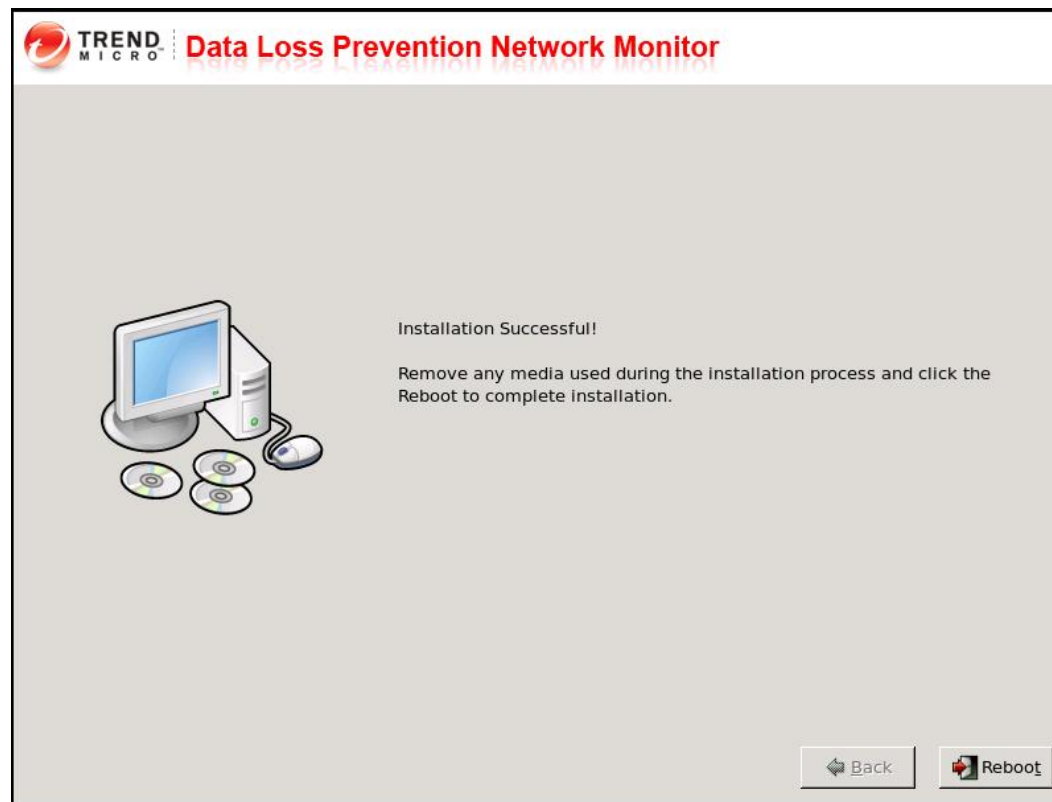
▶ NDLP的安装步骤



NDLP2.0介绍

▶ NDLP的安装步骤

- ▶ 安装完毕后，需要重启设备



NDLP2.0介绍

▶ NDLP的安装步骤

▶ 登陆NDLP的Linux命令行注册到DLP上

▶ *Clish*

▶ *Enable*

▶ *Configure dglink X.X.X*

```
*      Trend Micro Data Loss Prevention Network Monitor 2.0      *
*                                                                    *
*              WARNING: Authorized Access Only              *
*                                                                    *
*****

Welcome to DLPNM CLI. it is Sun May 15 15:14:47 CST 2011
> enable

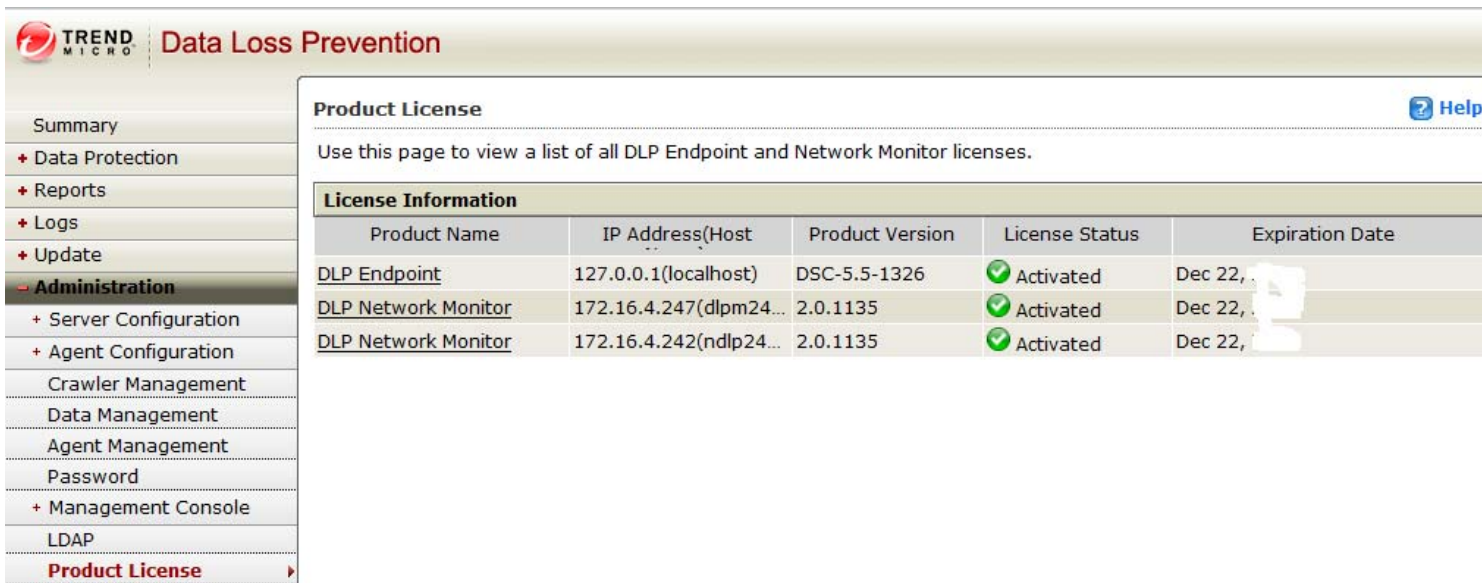
Entering privileged mode...
# configure
dglink      dns      gateway      hostname      interface
max_file_size password
# configure dglink ^

ip IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
# configure dglink 172.16.4.241
Ok to create fpga pattern : /tmp/fpga.tcp.ptn.raw
Ok to create fpga pattern : /tmp/fpga.udp.ptn.raw
# _
```

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 需激活NDLP



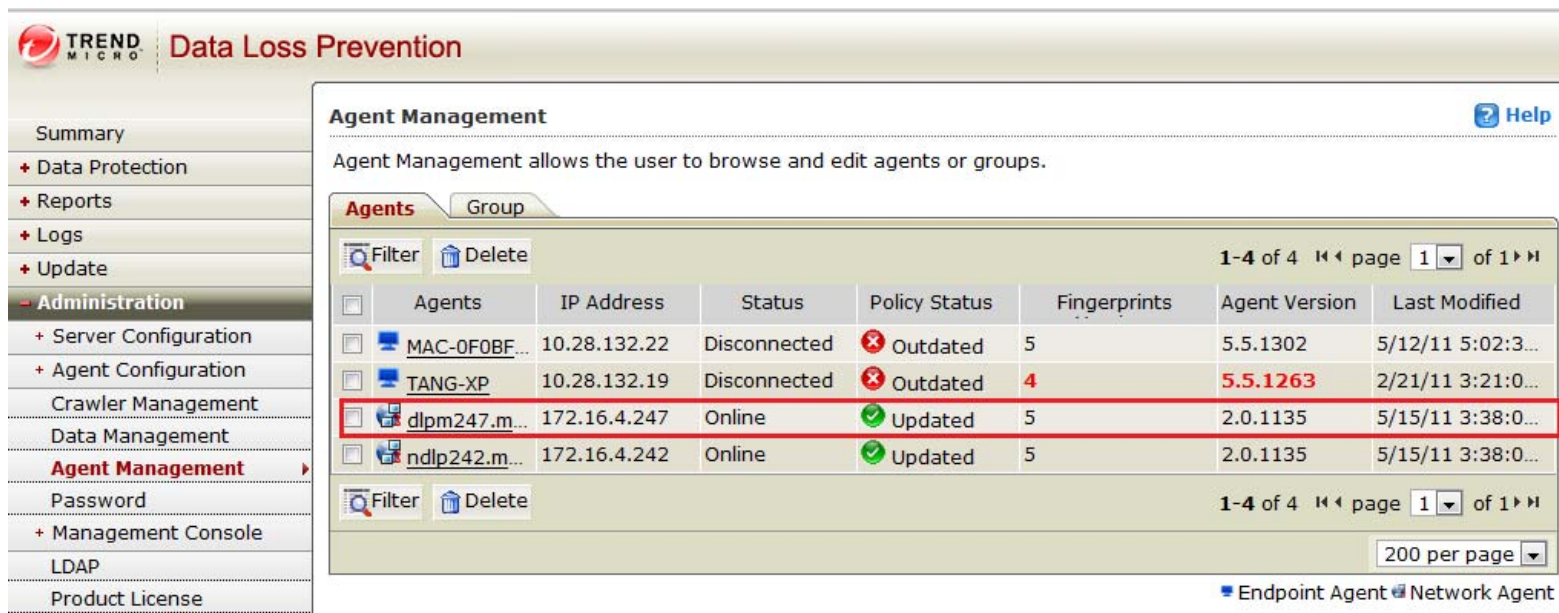
The screenshot displays the Trend Micro Data Loss Prevention (DLP) console interface. The top navigation bar includes the Trend Micro logo and the text "Data Loss Prevention". A left-hand navigation menu lists various administrative options, with "Administration" expanded to show "Product License" as the selected item. The main content area is titled "Product License" and includes a "Help" icon. Below the title, there is a descriptive text: "Use this page to view a list of all DLP Endpoint and Network Monitor licenses." A table titled "License Information" provides details for three licenses.

| Product Name | IP Address(Host) | Product Version | License Status | Expiration Date |
|-------------------------------------|-------------------------|-----------------|----------------|-----------------|
| DLP Endpoint | 127.0.0.1(localhost) | DSC-5.5-1326 | ✔ Activated | Dec 22, 2011 |
| DLP Network Monitor | 172.16.4.247(dlpm24...) | 2.0.1135 | ✔ Activated | Dec 22, 2011 |
| DLP Network Monitor | 172.16.4.242(ndlp24...) | 2.0.1135 | ✔ Activated | Dec 22, 2011 |

NDLP2.0介绍

▶ NDLP安装后的验证和使用

- ▶ 验证NDLP是否已经注册上，并Online状态



TREND MICRO Data Loss Prevention

Agent Management [Help](#)

Agent Management allows the user to browse and edit agents or groups.

Agents Group

Filter Delete 1-4 of 4 page 1 of 1

| Agents | IP Address | Status | Policy Status | Fingerprints | Agent Version | Last Modified |
|---------------------------------------|--------------|--------------|---------------|--------------|---------------|-------------------|
| <input type="checkbox"/> MAC-0F0BF... | 10.28.132.22 | Disconnected | ✘ Outdated | 5 | 5.5.1302 | 5/12/11 5:02:3... |
| <input type="checkbox"/> TANG-XP | 10.28.132.19 | Disconnected | ✘ Outdated | 4 | 5.5.1263 | 2/21/11 3:21:0... |
| <input type="checkbox"/> dlpm247.m... | 172.16.4.247 | Online | ✔ Updated | 5 | 2.0.1135 | 5/15/11 3:38:0... |
| <input type="checkbox"/> ndlp242.m... | 172.16.4.242 | Online | ✔ Updated | 5 | 2.0.1135 | 5/15/11 3:38:0... |

Filter Delete 1-4 of 4 page 1 of 1

200 per page

Endpoint Agent Network Agent

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 检查流量是否已经通过:

▶ 1、请将镜像口插入NDLP的端口

▶ 2、转到如下目录: `cd /opt/TrendMicro/ndlp/platform/QA`

▶ 执行 `./toe.sh`

```
Sun Dec 26 16:55:53 CST 2010
[STATISTICS]
syn_contrack:          1 (      184)
contrack_count:       1 (      154)
nr_pkscan_tx:         0 (     1125)
nr_btscan_tx:         0 (       202)
nr_fpga_err:          (         0)
nr_btscan_err:        (         0)
free_lowmem:          648M ( 200M/1011M)
nr_packet_bytes:      464 [  OM] -\
nr_pk_bytes:          0 [  OM] |
nr_bt_bytes:          0 [  OM] |
nr_tr_bytes:          0 [  OM] +- ( 550M)
nr_pages:             0 [  OM] --- (4096M)
nr_sb_drop:           0
nr_tr_drop:           0
nr_result_vy:         0          0
nr_result_vn:         202
nr_result_more:       0
nr_both_vn:           137
nr_timeout_hole:      0
nr_split:             0          0
nr_nonsplit:          91311
nr_flow_packets:      0
nr_flow_fifo:         0
nr_flow_pkscan:       0
nr_flow_btscan:       0
nr_in_conn:           1143      14260
nr_not_a_syn:         7          7
nr_corrupt:           31         1
nr_redirect:          0          0
overloading:          0 0 (1:0 fs:0 f:0 d:0)
===== [TCP_STATE] =====
SYN_SENT:             1 (         0)
SYN_RECV:             0 (         0)
ESTABLISHED:          0 (         0)
FIN_WAIT:             0 (         0)
CLOSE_WAIT:           0 (         0)
LAST_ACK:             1 (         0)
TIME_WAIT:            0 (         0)
CLOSE:                0 (         0)
█
```

NDLP2.0介绍

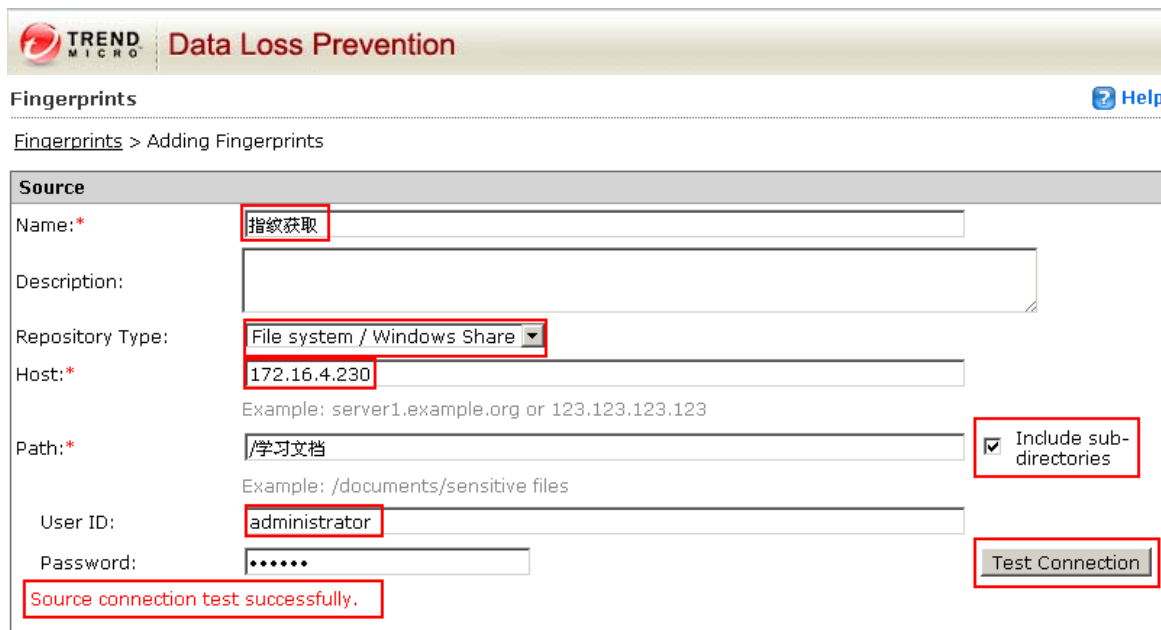
- ▶ *NDLP*安装后的验证和使用
 - ▶ 建立策略—与*DLP*常规使用类似
 - ▶ 可以分别建立如下条件：
 - ▶ **Fingerprints**指纹获取
 - ▶ **Pattern**设定
 - ▶ 关键字设定
 - ▶ 真实文件属性设定

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ Fingerprints指纹获取

▶ 方法一：共享方式获取



TREND MICRO Data Loss Prevention

Fingerprints [Help](#)

[Fingerprints](#) > Adding Fingerprints

Source

Name:* 指纹获取

Description:

Repository Type: File system / Windows Share

Host:* 172.16.4.230
Example: server1.example.org or 123.123.123.123

Path:* /学习文档 Include sub-directories
Example: /documents/sensitive files

User ID: administrator

Password: *****

Source connection test successfully.

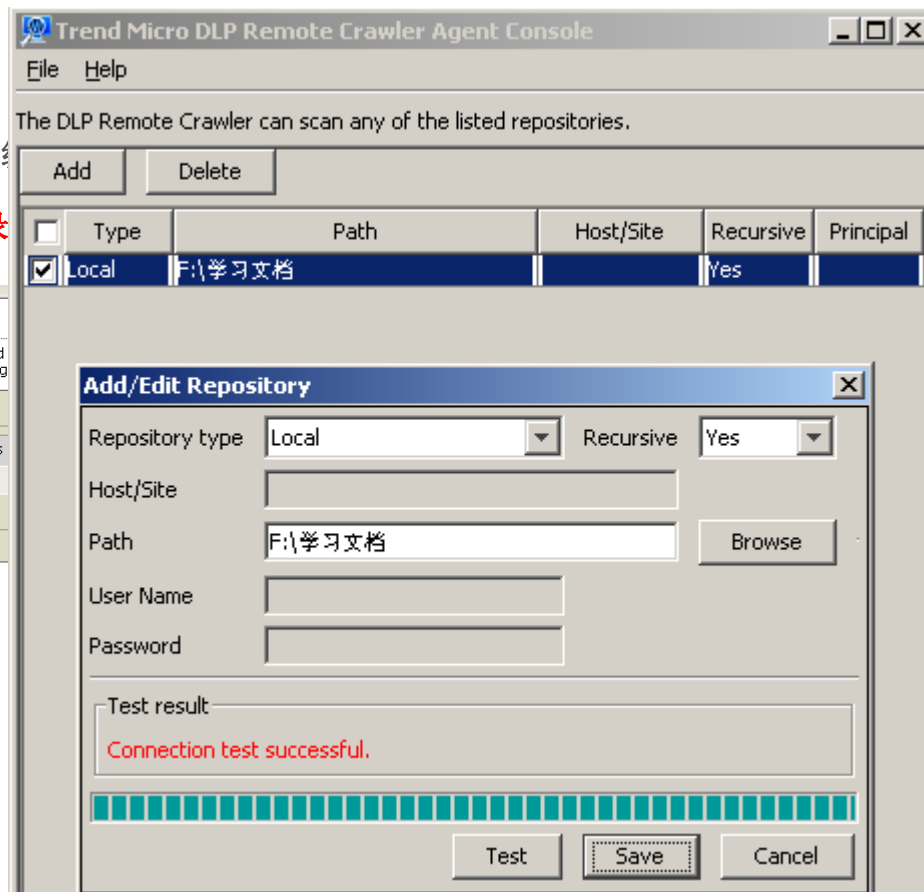
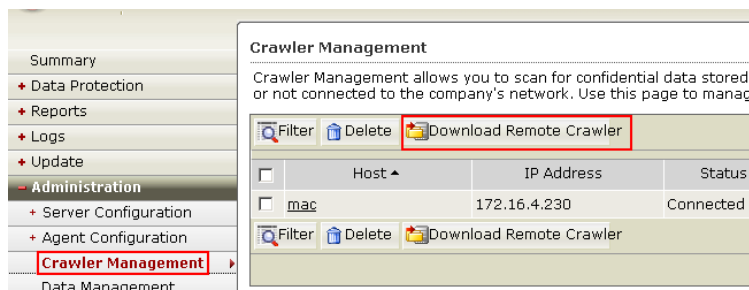
NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ Fingerprints指纹获取

▶ 方法一：通过Remote Crawler工具进行获取指纹

▶ 注意：此方式适用于存放需要保护数据目录



NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ Pattern设定

- ▶ Pattern设定是基于正则表达式完成。使DLP可以检测一些诸如身份证ID，银行卡号、家庭住址、电话号码等敏感信息外泄。默认已经设定一些条目，但大部分是参照国外使用方式进行设定，一般建议不使用此功能。



The screenshot shows the Trend Micro Data Loss Prevention (DLP) console interface. The left sidebar contains navigation options such as Summary, Data Protection, Digital Assets, Fingerprints, Patterns (highlighted), Keywords, File Attributes, Compliance Templates, Company Policies, Data Discovery, Device Control, Reports, Logs, Update, and Administration. The main content area is titled 'Patterns' and includes instructions to create patterns. A table lists several predefined patterns:

| <input type="checkbox"/> | Name | Description | Pattern | Last Modified |
|--------------------------|-----------------------|--------------------------------|---|-----------------------|
| <input type="checkbox"/> | ABA Routing Number | ABA Routing Number | [^\d]([0123678]\d{8})[^\d] | 11/12/10 2:41:19 A... |
| <input type="checkbox"/> | American Name | American people's name | [^\w]([A-Z][a-z]{1,12}\s?\s?[\s]?[A-... | 11/12/10 2:41:19 A... |
| <input type="checkbox"/> | Austria SSN | Austria SSN | [^\d](\d{4})\d{0[1-9]]1[0-2]\d{2}[... | 11/12/10 2:41:19 A... |
| <input type="checkbox"/> | Cal DL# /Cal ID# | CalID | [^\w-]([A-G]\d{7})[^\w-] | 11/12/10 2:41:19 A... |
| <input type="checkbox"/> | Canadian Social In... | Canadian Social Insurance N... | [^\w-]([1-79]\d{8})[1-79]\d{2}-\d{3}-\d... | 11/12/10 2:41:19 A... |
| <input type="checkbox"/> | China National ID | China National ID | [^\d-](\d{17})(\d x)[^\d-] | 11/12/10 2:41:19 A... |
| <input type="checkbox"/> | Credit Card Number | Credit Card Number | [^\d-](\d{15,16})\d{4}-\d{4}-\d{4}-\d{4}... | 11/12/10 2:41:19 A... |
| <input type="checkbox"/> | Danish Personal ID | Danish Personal ID | [^\d-](0[1-9])\d{12}3[01](0[1-9])1[0-2]... | 11/12/10 2:41:19 A... |

NDLP2.0介绍

▶ NDLP安装后的验证和使用

Keyword

 Help

▶ [Keyword](#) > Adding Keyword

Keywords

Name:*

Description:

Condition:

Import sub-keywords 未选择文件

Add/update sub-keywords

Sub-keyword

Name: Case Sensitive

Description:

Sub-keywords list

1-1 of 1 <<< page 1 of 1 >>>

| <input type="checkbox"/> | Name ▲ | Description | Case Sensitive | Last Modified Time |
|--------------------------|--------|-------------|------------------|--------------------|
| <input type="checkbox"/> | test | | Case Insensitive | |

1-1 of 1 <<< page 1 of 1 >>>

200 per page

行卡号

参照



Help



CST

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 文件属性设定

▶ 点击Data Protection--- **Digital** Assets---File Attributes， 右边点击Add

▶ 注意：**True file Attributes**采用识别真实文件类型属性，不是单纯的基于**File Attributes**

测。目前支持常见的**300**余种文件类型。当DLP识别某种类型的文件， [File Attributes](#) > Adding File Attributes

展名或者去除扩展名，DLP依旧可以有效的识别和检测。

The screenshot shows the Trend Micro Data Loss Prevention console. The left sidebar contains a navigation menu with options like Summary, Data Protection, Digital Assets, Fingerprints, Patterns, Keywords, File Attributes (highlighted), Compliance Templates, Company Policies, Data Discovery, and Device Control. The main content area is titled 'File Attributes' and includes a sub-header 'Trend Micro™ DLP Workflow'. Below this, there is a description: 'With File Attributes, you can block certain files from users that meet the criteria you have established.' There are three buttons: 'Add', 'Copy', and 'Delete'. Below the buttons is a table with the following data:

| <input type="checkbox"/> | Name | Description | Last Modified |
|--------------------------|--------------------|--------------------|-------------------------|
| <input type="checkbox"/> | Mac File Attribute | Mac File Attribute | 11/24/10 9:33:16 AM CST |
| <input type="checkbox"/> | 与得通讯 | | 12/20/10 5:22:20 PM CST |

At the bottom of the table, there are 'Add', 'Copy', and 'Delete' buttons, and a page indicator '1-2 of 2'.

The screenshot shows the 'Adding File Attributes' dialog box. It features a 'Select:' dropdown menu currently set to 'Selected types'. Below the dropdown is a list of file types, each with a checkbox and a dropdown arrow:

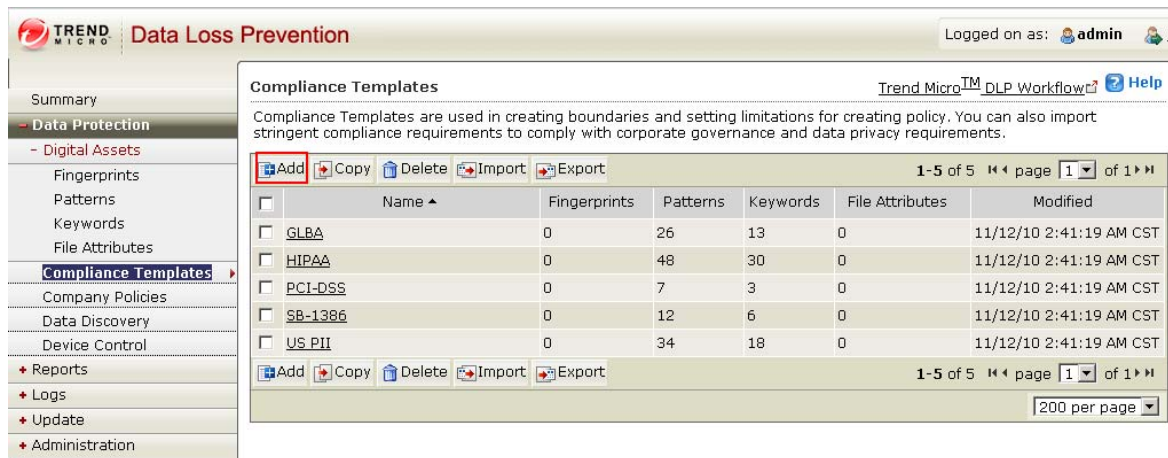
- Executable
- Document
- Image Document
- Graphic Document
- Multimedia
- Encapsulation Format
- Database Document
- Spreadsheet Document
- Presentation Document
- Desktop Publishing
- General Purpose Document
- Obfuscated File (Encrypted File)
- Others

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 建立合规模板

- ▶ 点击Data Protection--- [Compliance Templates](#), 右边点击Add



The screenshot shows the Trend Micro Data Loss Prevention (DLP) interface. The left sidebar contains a navigation menu with the following items: Summary, Data Protection (selected), Digital Assets, Fingerprints, Patterns, Keywords, File Attributes, Compliance Templates (highlighted), Company Policies, Data Discovery, Device Control, Reports, Logs, Update, and Administration. The main content area is titled 'Compliance Templates' and includes a description: 'Compliance Templates are used in creating boundaries and setting limitations for creating policy. You can also import stringent compliance requirements to comply with corporate governance and data privacy requirements.' Below the description is a table of templates with columns for Name, Fingerprints, Patterns, Keywords, File Attributes, and Modified. The 'Add' button is highlighted with a red box. The table contains five entries: GLBA, HIPAA, PCI-DSS, SB-1386, and US PII. The interface also shows a 'Logged on as: admin' status and a '200 per page' dropdown menu.

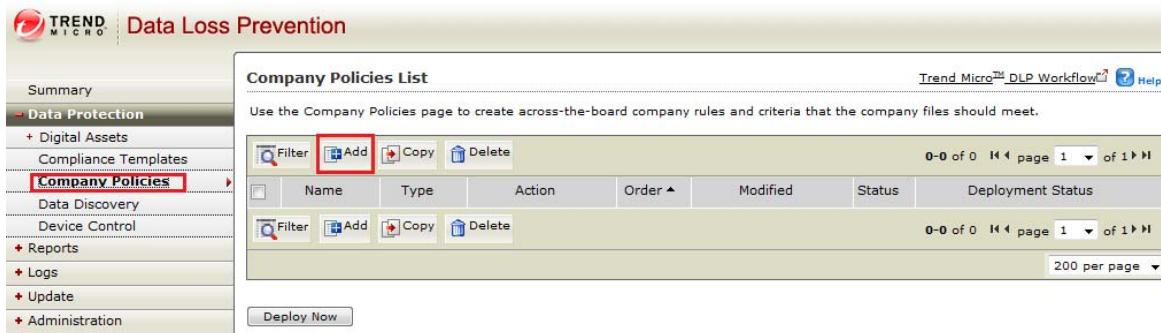
| <input type="checkbox"/> | Name ▲ | Fingerprints | Patterns | Keywords | File Attributes | Modified |
|--------------------------|---------|--------------|----------|----------|-----------------|-------------------------|
| <input type="checkbox"/> | GLBA | 0 | 26 | 13 | 0 | 11/12/10 2:41:19 AM CST |
| <input type="checkbox"/> | HIPAA | 0 | 48 | 30 | 0 | 11/12/10 2:41:19 AM CST |
| <input type="checkbox"/> | PCI-DSS | 0 | 7 | 3 | 0 | 11/12/10 2:41:19 AM CST |
| <input type="checkbox"/> | SB-1386 | 0 | 12 | 6 | 0 | 11/12/10 2:41:19 AM CST |
| <input type="checkbox"/> | US PII | 0 | 34 | 18 | 0 | 11/12/10 2:41:19 AM CST |

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 建立策略

▶ 点击Data Protection---Company Polices,右边点击Add

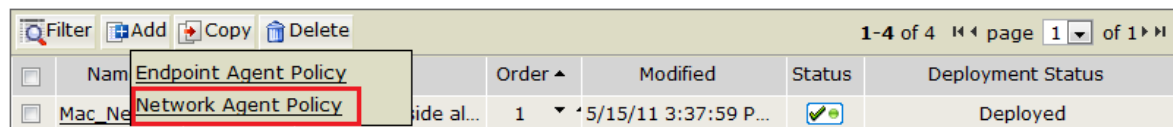


The screenshot shows the Trend Micro Data Loss Prevention interface. On the left is a navigation menu with 'Company Policies' selected. The main area is titled 'Company Policies List' and contains a table with columns: Name, Type, Action, Order, Modified, Status, and Deployment Status. The 'Add' button in the table's toolbar is highlighted with a red box.

Company Policies List

Trend Micro™ DLP Workflow Help

Use the Company Policies page to create across-the-board company rules and criteria that the company files should meet.



The screenshot shows the 'Company Policies List' table with two rows highlighted. The first row is 'Endpoint Agent Policy' and the second row is 'Network Agent Policy'.

| | Name | Type | Action | Order | Modified | Status | Deployment Status |
|--------------------------|-----------------------------------|------------|--------|-------|----------------------|--------|-------------------|
| <input type="checkbox"/> | Endpoint Agent Policy | | | | | | |
| <input type="checkbox"/> | Mac_Ne... Network Agent Policy | side al... | | 1 | 5/15/11 3:37:59 P... | | Deployed |

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 建立策略

▶ 选择需要监控的网段:

Policy List - Edit [Help](#)

Policy List > Mac_NetWork_Policy

The updated policy was deployed. If you make additional changes to this policy, you must redeploy it.

Target Channel Condition Action

Policy Name:

Policy Order:

Target

Select by:

Input:

Example, IP address/subnet mask, or IP address.

Selected:

From

All IP Addresses

Exception

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 建立策略

▶ 选择需要监控的管道:

▶ NDLP支持如下管道:

▶ Email

▶ FTP

▶ HTTP

▶ IM

▶ SMB

▶ Web Mail

▶ 并可以根据需要输入自定义白名单

Policy List - Edit Help

Policy List > Mac_NetWork_Policy

The updated policy was deployed. If you make additional changes to this policy, you must redeploy it.

Target Channel Condition Action

Check to prevent users from accessing sensitive information with the following:

Channels

Email

SMTP Email

Approved domain names

Separate multiple domain names with a comma. (Example: admin@yahoo.com,admin@gmail.com)

FTP

Approved FQDN or IP addresses

Separate multiple FQDN or IP address ranges with a comma. (Example: ftp.trendmicro.com,192.168.2.1/10)

HTTP

Approved FQDN or IP addresses

Separate multiple FQDN or IP address ranges with a comma. (Example: trendmicro.com,192.168.2.1/10)

Instant Messengers

IM AIM
IM MSN
IM Yahoo! Messenger

SMB

Web Mail

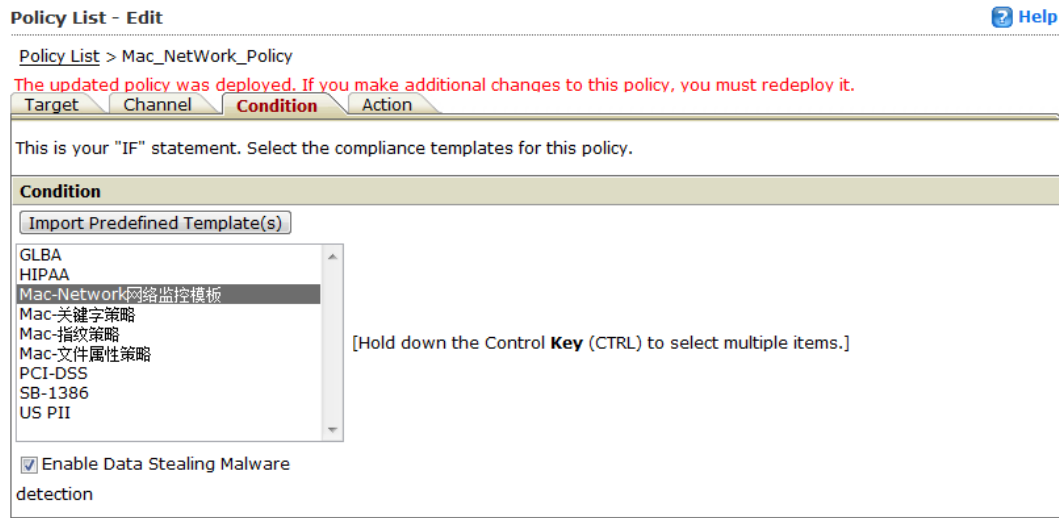
Web Mail (GMail)
Web Mail (HotMail)
Web Mail (Yahoo!Mail)

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 建立策略

▶ 选择需要使用的模板:



The screenshot shows the 'Policy List - Edit' window for 'Mac_NetWork_Policy'. The 'Condition' tab is active, displaying a list of predefined templates. The 'Mac-Network网络监控模板' is selected. Below the list, there is a checkbox for 'Enable Data Stealing Malware detection' which is checked.

Policy List - Edit Help

Policy List > Mac_NetWork_Policy

The updated policy was deployed. If you make additional changes to this policy, you must redeploy it.

Target Channel **Condition** Action

This is your "IF" statement. Select the compliance templates for this policy.

Condition

Import Predefined Template(s)

- GLBA
- HIPAA
- Mac-Network网络监控模板
- Mac-关键字策略
- Mac-指纹策略
- Mac-文件属性策略
- PCI-DSS
- SB-1386
- US PII

[Hold down the Control **Key** (CTRL) to select multiple items.]

Enable Data Stealing Malware detection

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 建立策略

▶ 选择处理措施:

- ▶ Local Area Network ---边界出局域网
- ▶ Local Machine----边界为出本机

▶ 注意: NDLP只有监控, 不会拦截作用。

Policy List - Edit

[Help](#)

[Policy List](#) > Mac_NetWork_Policy

The updated policy was deployed. If you make additional changes to this policy, you must redeploy it.

| Target | Channel | Condition | Action |
|---|---------|-----------|--------|
| Specify the actions for this policy. | | | |
| Network Boundary | | | |
| Network Agents | | | |
| <input type="radio"/> Local Area Network (recommended) ⓘ | | | |
| <input checked="" type="radio"/> Local Machine (strict filtering) ⓘ | | | |
| System Action | | | |
| Actions to take: | | | |
| <input checked="" type="checkbox"/> Log | | | |
| <input checked="" type="checkbox"/> Server side alerting | | | |
| <input type="checkbox"/> Forensic data capturing | | | |

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 建立策略

▶ 选择处理措施:

- ▶ **Local Area Network** ---边界出局域网
- ▶ **Local Machine**----边界为出本机

▶ 注意: NDLP只有监控, 不会拦截作用。

Policy List - Edit

[? Help](#)

[Policy List](#) > [Mac_NetWork_Policy](#)

The updated policy was deployed. If you make additional changes to this policy, you must redeploy it.

| Target | Channel | Condition | Action |
|---|---------|-----------|--------|
| Specify the actions for this policy. | | | |
| Network Boundary | | | |
| Network Agents | | | |
| <input type="radio"/> Local Area Network (recommended) ⓘ | | | |
| <input checked="" type="radio"/> Local Machine (strict filtering) ⓘ | | | |
| System Action | | | |
| Actions to take: | | | |
| <input checked="" type="checkbox"/> Log | | | |
| <input checked="" type="checkbox"/> Server side alerting | | | |
| <input type="checkbox"/> Forensic data capturing | | | |

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 建立策略

▶ 选择处理措施:

- ▶ Local Area Network ---边界出局域网
- ▶ Local Machine----边界为出本机

▶ 注意: NDLP只有监控, 不会拦截作用。

Policy List - Edit

[? Help](#)

[Policy List](#) > [Mac_NetWork_Policy](#)

The updated policy was deployed. If you make additional changes to this policy, you must redeploy it.

| Target | Channel | Condition | Action |
|---|---------|-----------|--------|
| Specify the actions for this policy. | | | |
| Network Boundary | | | |
| Network Agents | | | |
| <input type="radio"/> Local Area Network (recommended) ⓘ | | | |
| <input checked="" type="radio"/> Local Machine (strict filtering) ⓘ | | | |
| System Action | | | |
| Actions to take: | | | |
| <input checked="" type="checkbox"/> Log | | | |
| <input checked="" type="checkbox"/> Server side alerting | | | |
| <input type="checkbox"/> Forensic data capturing | | | |

NDLP2.0介绍

▶ NDLP安装后的验证和使用

▶ 检测测试

▶ 通过共享方式，传一个mac.txt，内容为：trendtrend

Log Query Trend Micro™ DLP Workflow [Help](#)

Query [Hide Query]

Data Range: Today From 12:00 To 12:00

Log Type: Policy Deployment Security Violations Server Status System Events Security Audit

Filter Export Refresh 1-200 of 1601 page 1 of 9

| Security Violations | | | | | | | | | |
|---------------------------------|------|---------------------------|---------|--------|---------|---------|---------------|----------|-------------------|
| ID | User | Department | Host | Domain | Channel | Offline | Destination | Forensic | Date |
| 31... | N/A | | dlp2... | N/A | SMB | No | 10.28.132.121 | | 5/15/11 5:09:0... |
| Source IP | | 172.16.4.101 | | | | | | | |
| Desination IP | | 10.28.132.121 | | | | | | | |
| Document Path: | | trend.txt | | | | | | | |
| Content Type: | | text | | | | | | | |
| Content: | | trendtrend | | | | | | | |
| Matched Doc Path: | | N/A | | | | | | | |
| Policy Name: | | Mac_NetWork_Policy | | | | | | | |
| Compliance Template/DSM: | | Mac-Network网络监控模板 | | | | | | | |
| Action: | | Log;Server side alerting; | | | | | | | |

NDLP2.0介绍

▶ NDLP常见问题和解决



- ▶ 问题一：DLP Server控制台上看不到NDLP，或者显示状态“Disconnect”
 - ▶ 检查NDLP设备的管理口是否连接正确
 - ▶ 只有板载第一口（eth0）为管理口
 - ▶ 网络设定是否正确，可以在clish中输入：**show network**
 - ▶ 使用ping命令，检查与DLP Server的通信连接

```
> show network
Host name: dlpm247.mac.com
Management IP Setting
  Type: static
  IP Address: 172.16.4.247
  Netmask: 255.255.255.0
  Default gateway: 172.16.4.1
  DNS Server 1: 10.28.132.101
  DNS Server 2:
Interfaces information:
eth0: Speed 1000Mb/s, Duplex Full, Auto-negotiation on
eth1: Speed 1000Mb/s, Duplex Full, Auto-negotiation on
eth2: Speed 1000Mb/s, Duplex Full, Auto-negotiation on
eth3: Speed 1000Mb/s, Duplex Full, Auto-negotiation on
DLP Controller:
  IP Address: 172.16.4.241
```

NDLP2.0介绍

▶ NDLP常见问题和解决

- ▶ 问题二：DLP Server控制台上显示NDLP策略outdate或者Fingerprint版本错误

| | | | | | | |
|--|--------------|--------------|--|---|----------|-------------------|
|  ndlp242.m... | 172.16.4.242 | Disconnected |  Outdated | 5 | 2.0.1135 | 5/15/11 4:57:0... |
|--|--------------|--------------|--|---|----------|-------------------|

- ▶ 检查NDLP设备的管理口是否连接正确
- ▶ 检查策略是否部署到NDLP上（通过时间戳验证）
- ▶ 策略文件路径：*/root/prod/sensorSDK/data/tmpe.pol*
- ▶ 指纹文件路径：
 - ▶ */root/prod/sensorSDK/data/repo/sig_table.smeta*
 - ▶ */root/prod/sensorSDK/data/repo/sig_table.stbl*

NDLP2.0介绍

▶ NDLP常见问题和解决

- ▶ 问题三：DLP Server控制台上没有任何日志
 - ▶ 检查NDLP设备的管理口是否连接正确
 - ▶ 检查镜像口是否有正常数据
 - ▶ 检查策略是否部署正确，注意：*boundary*边界设定，是否有*Proxy*代理服务器

NDLP2.0介绍

▶ NDLP常见问题和解决

▶ 问题三: *DLP Server*流量是否过载

▶ 使用脚本工具进行检测: */opt/TrendMicro/ndlp/platform/QA_TOOLS*

```
[root@d1pm247 QA_TOOLS]# pwd
/opt/TrendMicro/ndlp/platform/QA_TOOLS
[root@d1pm247 QA_TOOLS]# ll
total 32
-rwxr-xr-x 1 root root 50 Nov 2 2010 df.sh
-rwxr-xr-x 1 root root 217 Nov 2 2010 fse.sh
-rwxr-xr-x 1 root root 85 Nov 2 2010 mem.sh
-rwxr-xr-x 1 root root 217 Nov 2 2010 toe.sh
```

