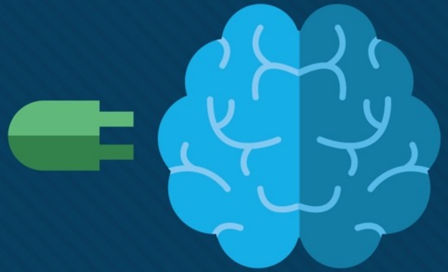
Module 10: LAN Security Concepts

Instructor Materials

Switching, Routing and Wireless
Essentials v7.0 (SRWE)



Module Objectives

Module Title: LAN Security Concepts

Module Objective: Explain how vulnerabilities compromise LAN security

Topic Title	Topic Objective
Endpoint Security	Explain how to use endpoint security to mitigate attacks
Access Control	Explain how AAA and 802.1x are used to authenticate LAN endpoints and devices
Layer 2 Security Threats	Identify Layer 2 vulnerabilities
MAC Address Table Attack	Explain how a MAC address table attack compromised LAN security
LAN Attacks	Explain how LAN attacks compromise LAN security

10.1 Endpoint Security

Network Attacks Today

The news media commonly covers attacks on enterprise networks. Simply search the internet for “latest network attacks” to find up-to-date information on current attacks. Most likely, these attacks will involve one or more of the following:

- **Distributed Denial of Service (DDoS)** – This is a coordinated attack from many devices, called zombies, with the intention of degrading or halting public access to an organization’s website and resources.
- **Data Breach** – This is an attack in which an organization’s data servers or hosts are compromised to steal confidential information.
- **Malware** – This is an attack in which an organization’s hosts are infected with malicious software that cause a variety of problems. For example, ransomware such as WannaCry encrypts the data on a host and locks access to it until a ransom is paid.

Network Security Devices

Various network security devices are required to protect the network perimeter from outside access. These devices could include the following:

- Virtual Private Network (VPN) enabled router - provides a secure connection to remote users across a public network and into the enterprise network. VPN services can be integrated into the firewall.
- Next-Generation Firewall (NGFW) - provides stateful packet inspection, application visibility and control, a next-generation intrusion prevention system (NGIPS), advanced malware protection (AMP), and URL filtering.
- Network Access Control (NAC) - includes authentication, authorization, and accounting (AAA) services. In larger enterprises, these services might be incorporated into an appliance that can manage access policies across a wide variety of users and device types. The Cisco Identity Services Engine (ISE) is an example of a NAC device.

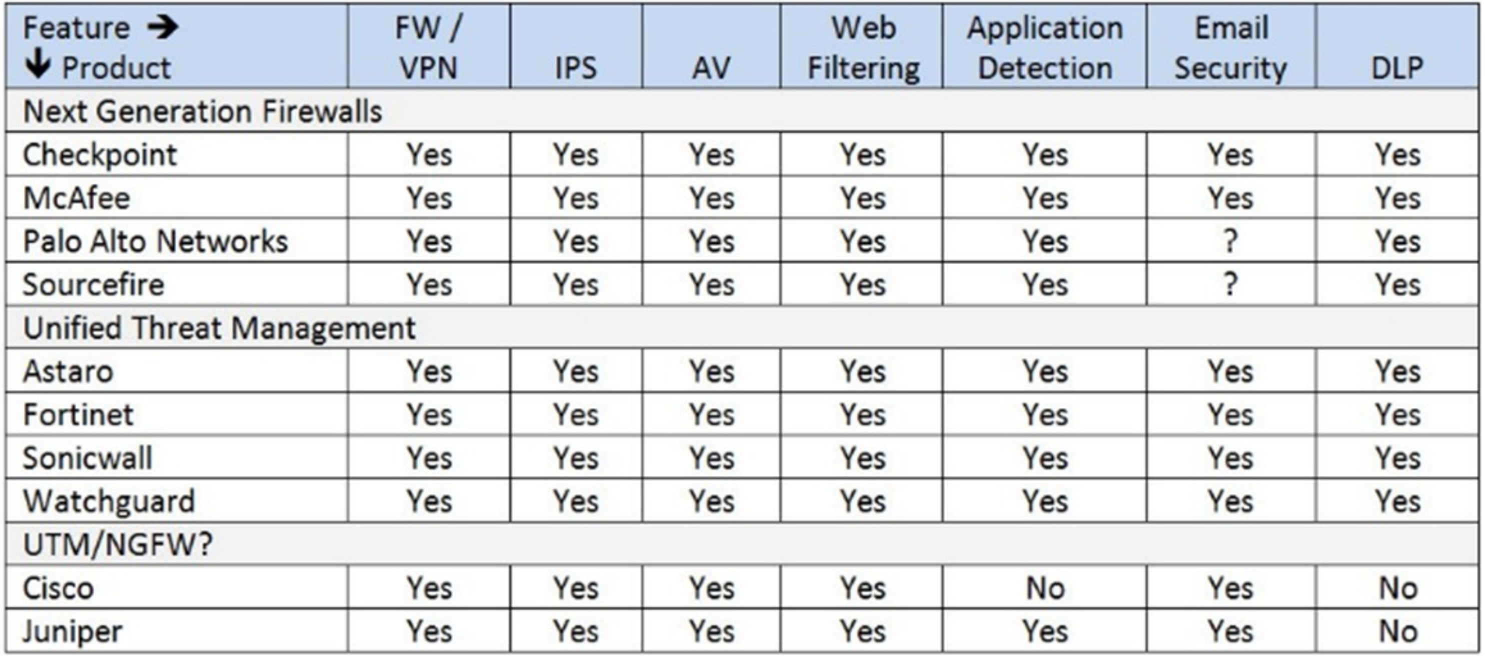
Dodatečné funkce mění firewall v UTM resp. NGFW

- tunelování
- translace adres
- autentizace uživatelů
- detekce průniků
- blokace, restrikce a antivirový nástroj
- podpora demilitarizovaného portu
- vzdálené řízení nastavování
- alarmy
- kešování informací atd.

UTM (unified threat management) a NGFW (nextgen FW)

- **UTM** byly původně firewally kategorie SMB rozšířené o funkce IDS/IPS, antimalwaru, antispamu a filtrování obsahu v jediném snadno spravovatelném zařízení. Nověji přidaly funkce, jako je VPN, vyvažování zátěže a prevence ztráty dat (DLP), a jsou stále častěji dodávány jako služba prostřednictvím cloudu.
- **NGFW** kombinují tradiční filtrování portů a protokolů s funkcemi IDS/IPS a schopností detekovat provoz na aplikační vrstvě; postupem času přidali další funkce, jako je hloubková kontrola paketů a detekce malwaru.
- Ochrana proti malwaru a virům, webový proxy a další, které existují v bráně firewall UTM, nejsou původní součástí architektury NGFW, protože tyto linie byly původně outsourcovány a odstraněny, což zajistilo bohaté stupně škálovatelnosti pro velká prostředí.

Výrobci NGEW a UTM



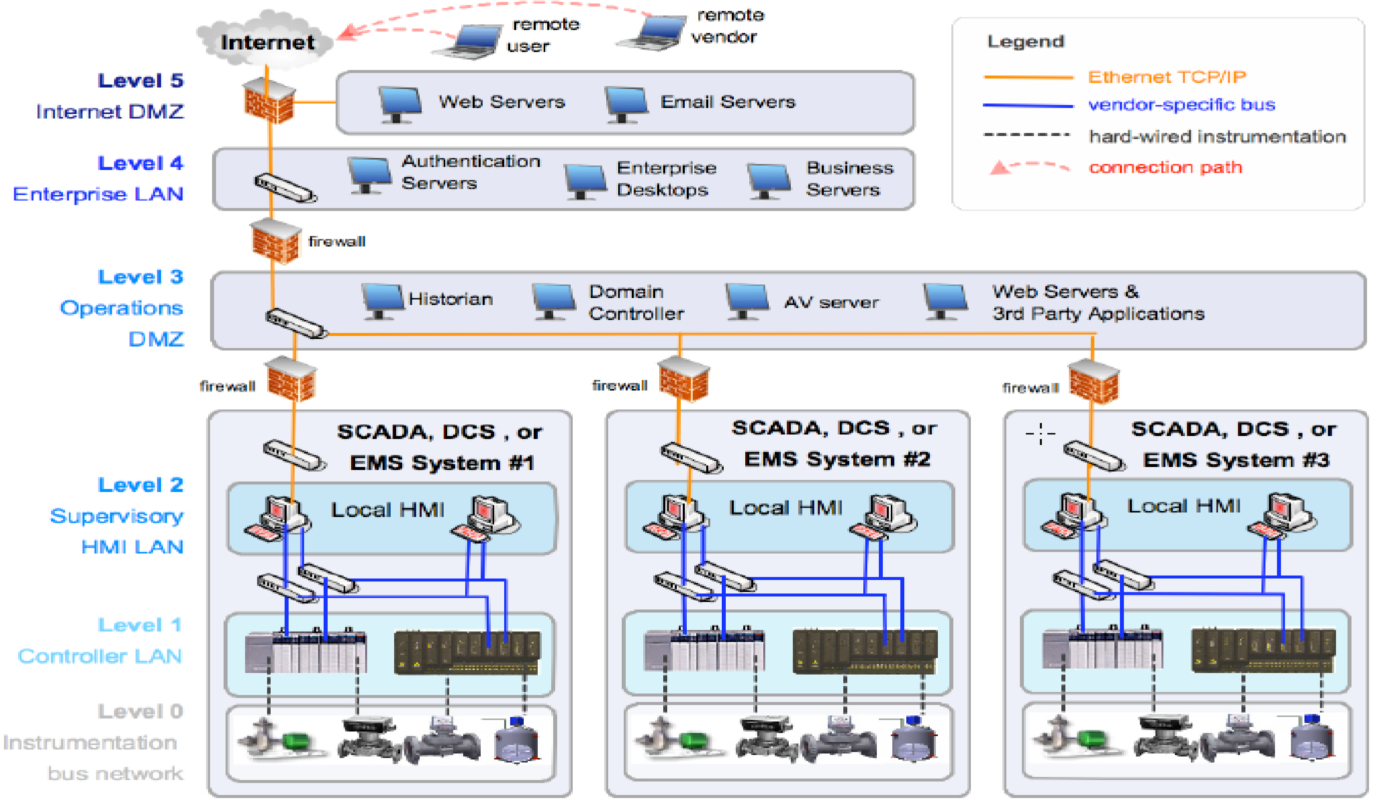
Feature → ↓ Product	FW / VPN	IPS	AV	Web Filtering	Application Detection	Email Security	DLP
Next Generation Firewalls							
Checkpoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes
McAfee	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Palo Alto Networks	Yes	Yes	Yes	Yes	Yes	?	Yes
Sourcefire	Yes	Yes	Yes	Yes	Yes	?	Yes
Unified Threat Management							
Astaro	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fortinet	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Sonicwall	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Watchguard	Yes	Yes	Yes	Yes	Yes	Yes	Yes
UTM/NGFW?							
Cisco	Yes	Yes	Yes	Yes	No	Yes	No
Juniper	Yes	Yes	Yes	Yes	Yes	Yes	No

Obrana průmyslových zařízení pomocí zónové obrany

- Speciální firewally (conduits) mají pomocí seznamů povolených příkazů zabránit přelévání problémů z jedné zóny do druhé. Řada od sebe oddělených zón umožňuje realizovat tzv. obranu v hloubce.

- Typickým conduitem je např. Tofino Security Appliance (TSA).

Příklad rozdělení řízení elektrárny do jednotlivých úrovní



Internet

remote user

remote vendor

Legend

- Ethernet TCP/IP
- vendor-specific bus
- hard-wired instrumentation
- connection path

Level 5
Internet DMZ

Web Servers
Email Servers

Level 4
Enterprise LAN

Authentication Servers
Enterprise Desktops
Business Servers

firewall

Level 3
Operations
DMZ

Historian
Domain Controller
AV server
Web Servers & 3rd Party Applications

firewall

SCADA, DCS , or EMS System #1

SCADA, DCS , or EMS System #2

SCADA, DCS , or EMS System #3

Level 2
Supervisory
HMI LAN

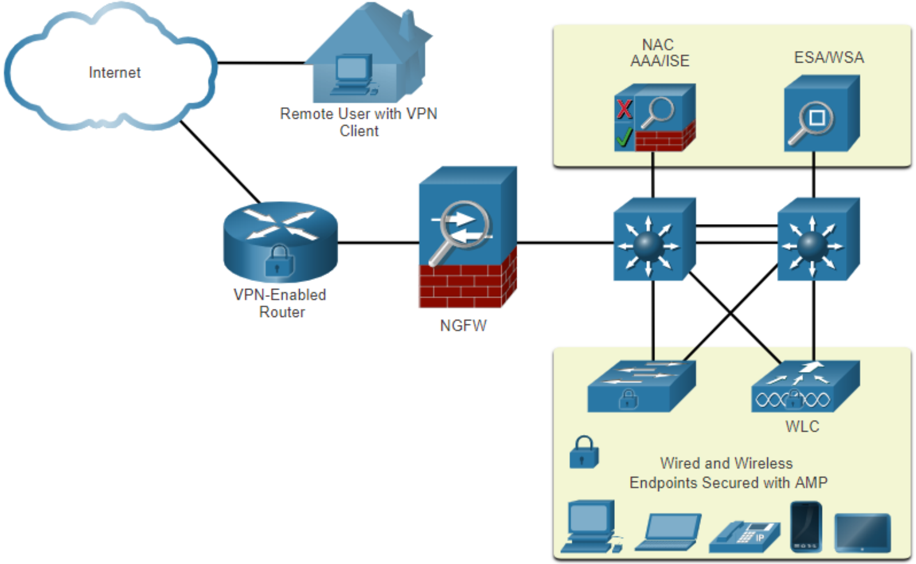
Local HMI

Level 1
Controller LAN

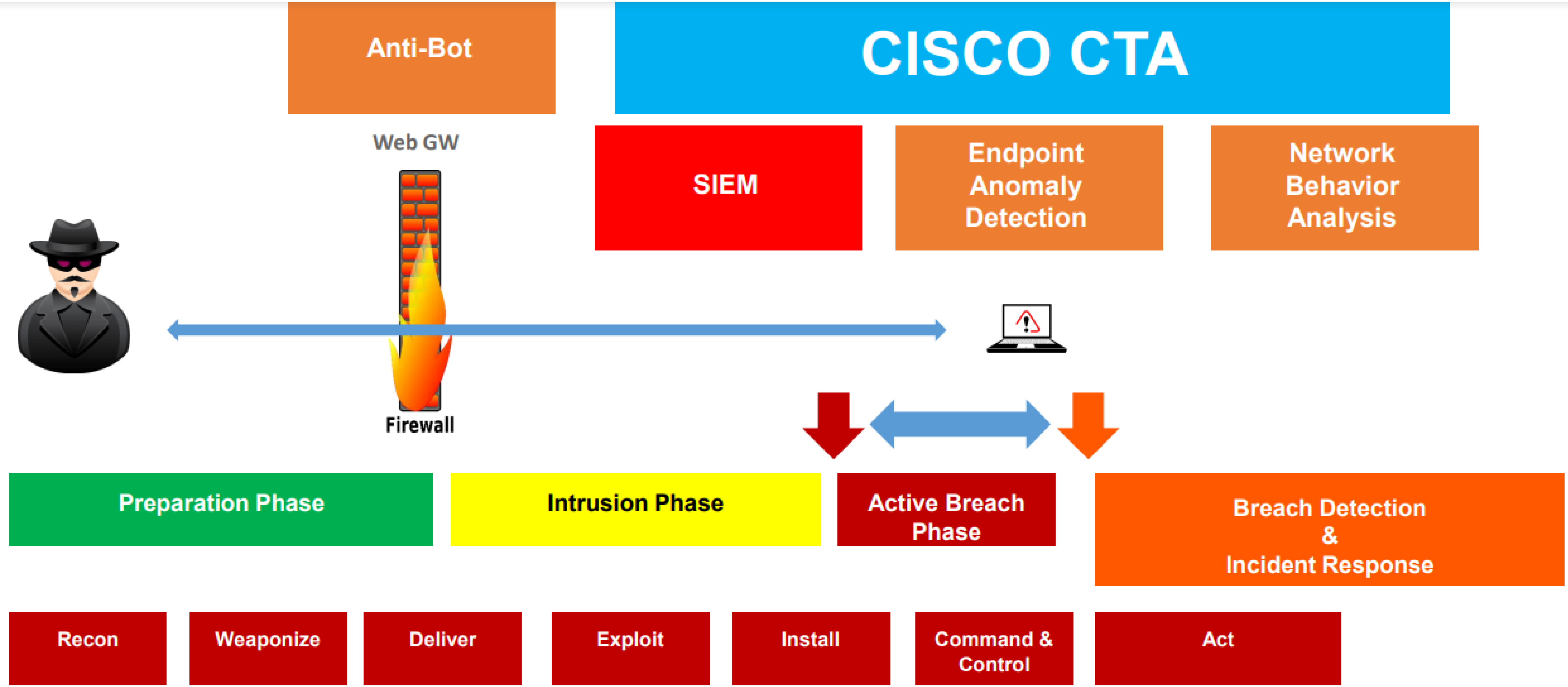
Level 0
Instrumentation
bus network

Endpoint Protection

- Endpoints are hosts which commonly consist of laptops, desktops, servers, and IP phones, as well as employee-owned devices. Endpoints are particularly susceptible to malware-related attacks that originate through email or web browsing.
- Endpoints have typically used traditional host-based security features, such as antivirus/antimalware, host-based firewalls, and host-based intrusion prevention systems (HIPSs).
- Endpoints today are best protected by a combination of NAC, AMP software, an email security appliance (ESA), and a web security appliance (WSA).


Internet
Remote User with VPN Client
VPN-Enabled Router
NGFW
NAC AAA/ISE
ESA/WSA
WLC
Wired and Wireless Endpoints Secured with AMP

CISCO Cognitive Threat Analytics (CTA), pak Cognitive Intelligence nakonec naintegrováno do Cisco Secure Endpoint (AMP for Endpoints)



Anti-Bot

CISCO CTA

Web GW

SIEM

Endpoint Anomaly Detection

Network Behavior Analysis

Firewall

Preparation Phase

Intrusion Phase

Active Breach Phase

Breach Detection & Incident Response

Recon

Weaponize

Deliver

Exploit

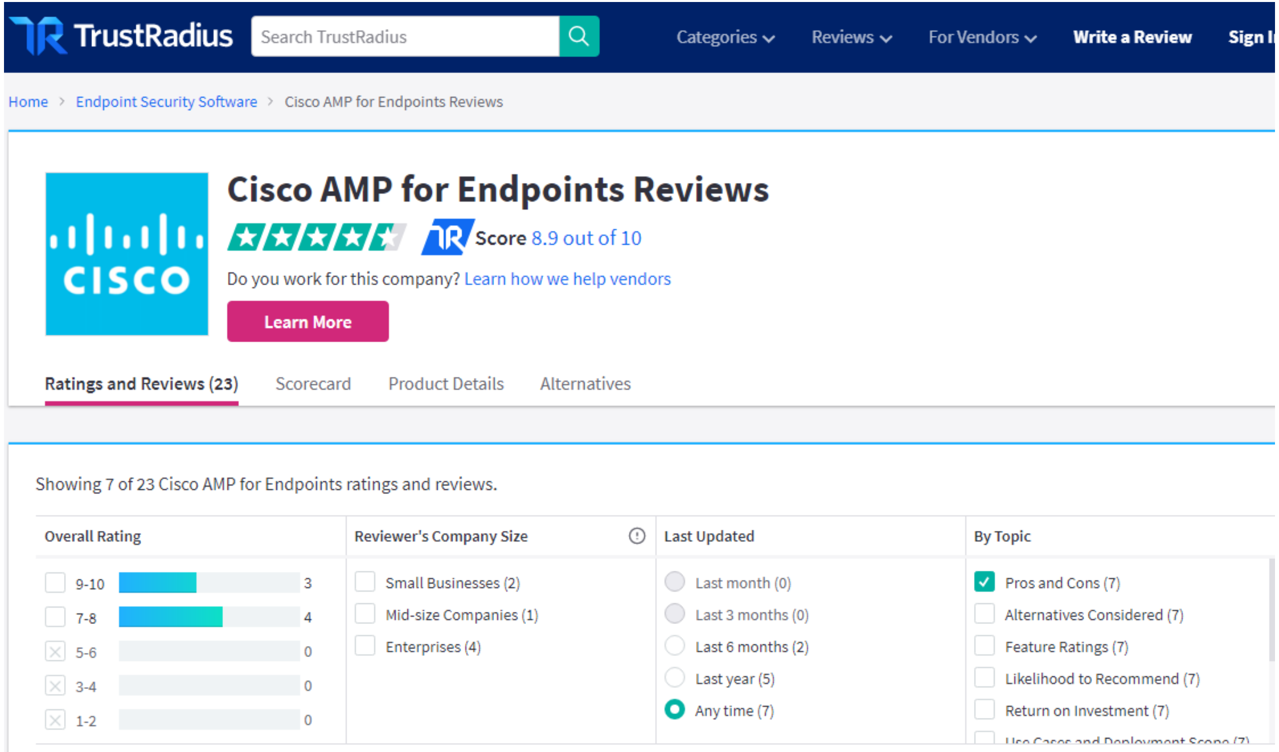
Install

Command & Control

Act

Hodnocení Cisco AMP

https://www.trustradius.com/endpoint-security



TrustRadius Search TrustRadius Categories Reviews For Vendors **Write a Review** **Sign I**

Home › Endpoint Security Software › Cisco AMP for Endpoints Reviews

Cisco AMP for Endpoints Reviews

Score 8.9 out of 10

Do you work for this company? Learn how we help vendors

Learn More

Ratings and Reviews (23) Scorecard Product Details Alternatives

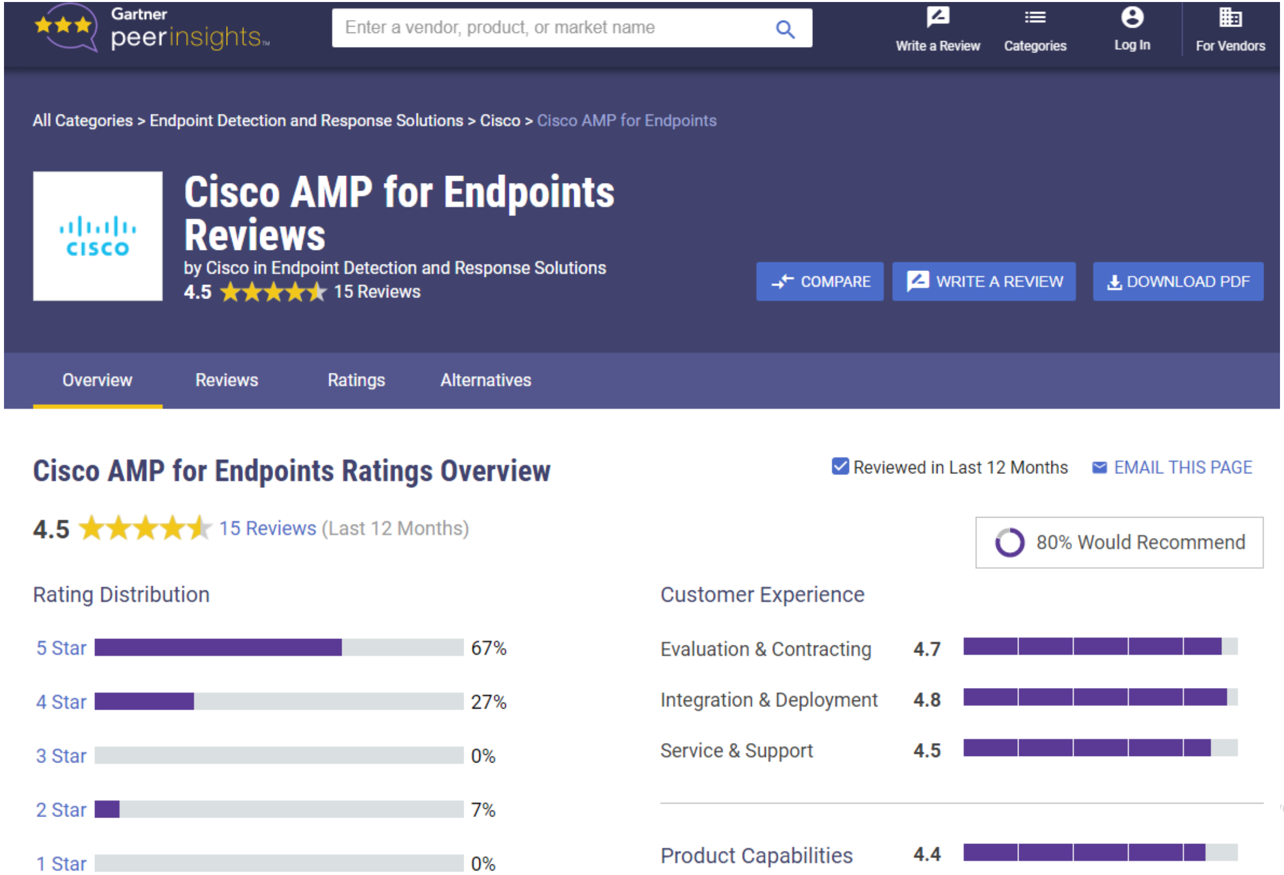
Showing 7 of 23 Cisco AMP for Endpoints ratings and reviews.

Overall Rating		Reviewer's Company Size	Last Updated	By Topic
□ 9-10	3	□ Small Businesses (2)	○ Last month (0)	☑ Pros and Cons (7)
□ 7-8	4	□ Mid-size Companies (1)	○ Last 3 months (0)	□ Alternatives Considered (7)
☒ 5-6	0	□ Enterprises (4)	○ Last 6 months (2)	□ Feature Ratings (7)
☒ 3-4	0		○ Last year (5)	□ Likelihood to Recommend (7)
☒ 1-2	0		● Any time (7)	□ Return on Investment (7)
				□ Use Cases and Deployment Scope (7)

Nejlépe hodnocené produkty nejsou od Cisco: Sophos Intercept X, FortiClient, Bitdefender GravityZone a Symantec Endpoint Security.

Hodnocení u Gartnera

https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions/vendor/cisco/product/cisco-amp-for-endpoints



All Categories > Endpoint Detection and Response Solutions > Cisco > Cisco AMP for Endpoints

Cisco AMP for Endpoints Reviews

by Cisco in Endpoint Detection and Response Solutions

4.5 ★★★★½ 15 Reviews

Cisco AMP for Endpoints Ratings Overview

☑ Reviewed in Last 12 Months

EMAIL THIS PAGE

4.5 ★★★★½ 15 Reviews (Last 12 Months)

80% Would Recommend

Rating Distribution

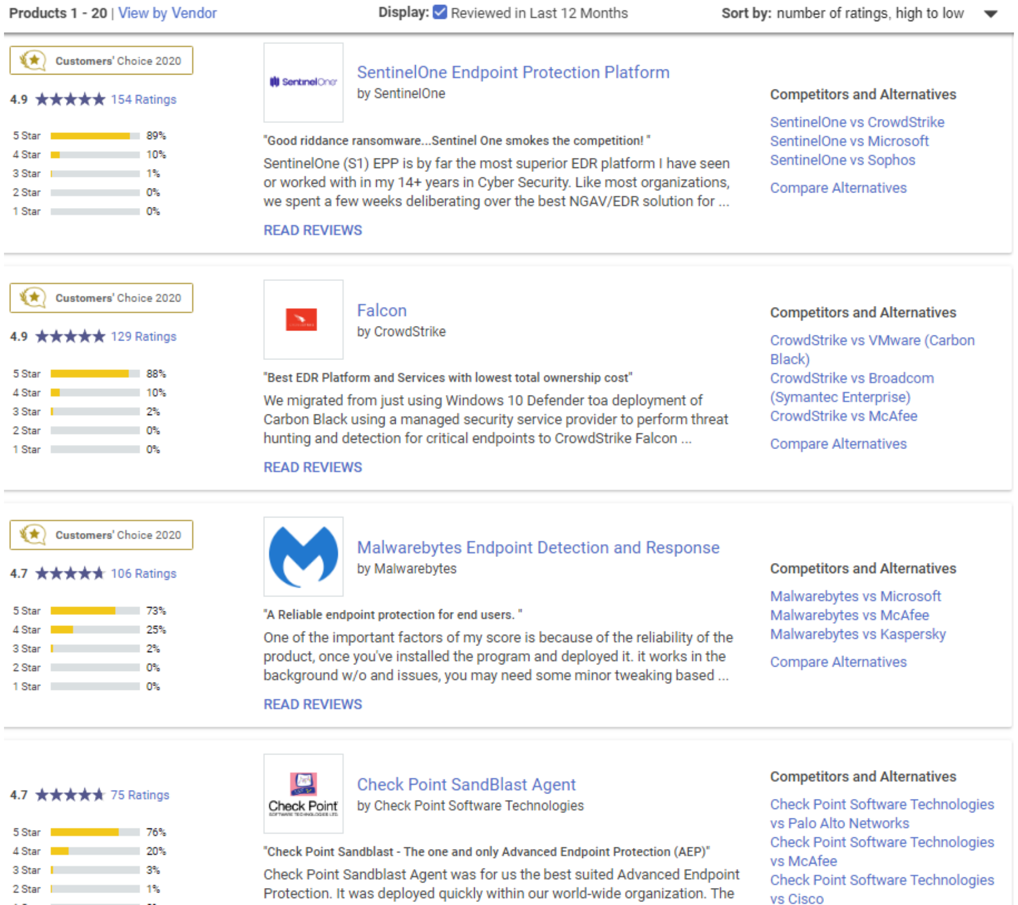
5 Star	67%
4 Star	27%
3 Star	0%
2 Star	7%
1 Star	0%

Customer Experience

Evaluation & Contracting	4.7
Integration & Deployment	4.8
Service & Support	4.5

Product Capabilities	4.4

Nejlépe hodnocené starší produkty dle Gartnera



Products 1 - 20 | View by Vendor Display: ☑ Reviewed in Last 12 Months Sort by: number of ratings, high to low

Customers' Choice 2020

4.9 ★★★★★ 154 Ratings

5 Star	89%
4 Star	10%
3 Star	1%
2 Star	0%
1 Star	0%

SentinelOne Endpoint Protection Platform
by SentinelOne

"Good riddance ransomware...Sentinel One smokes the competition! "

SentinelOne (S1) EPP is by far the most superior EDR platform I have seen or worked with in my 14+ years in Cyber Security. Like most organizations, we spent a few weeks deliberating over the best NGAV/EDR solution for ...

READ REVIEWS

Competitors and Alternatives

SentinelOne vs CrowdStrike
SentinelOne vs Microsoft
SentinelOne vs Sophos

Compare Alternatives

Customers' Choice 2020

4.9 ★★★★★ 129 Ratings

5 Star	88%
4 Star	10%
3 Star	2%
2 Star	0%
1 Star	0%

Falcon
by CrowdStrike

"Best EDR Platform and Services with lowest total ownership cost"

We migrated from just using Windows 10 Defender toa deployment of Carbon Black using a managed security service provider to perform threat hunting and detection for critical endpoints to CrowdStrike Falcon ...

READ REVIEWS

Competitors and Alternatives

CrowdStrike vs VMware (Carbon Black)
CrowdStrike vs Broadcom (Symantec Enterprise)
CrowdStrike vs McAfee

Compare Alternatives

Customers' Choice 2020

4.7 ★★★★★ 106 Ratings

5 Star	73%
4 Star	25%
3 Star	2%
2 Star	0%
1 Star	0%

Malwarebytes Endpoint Detection and Response
by Malwarebytes

"A Reliable endpoint protection for end users. "

One of the important factors of my score is because of the reliability of the product, once you've installed the program and deployed it. it works in the background w/o and issues, you may need some minor tweaking based ...

READ REVIEWS

Competitors and Alternatives

Malwarebytes vs Microsoft
Malwarebytes vs McAfee
Malwarebytes vs Kaspersky

Compare Alternatives

4.7 ★★★★★ 75 Ratings

5 Star	76%
4 Star	20%
3 Star	3%
2 Star	1%

Check Point SandBlast Agent
by Check Point Software Technologies

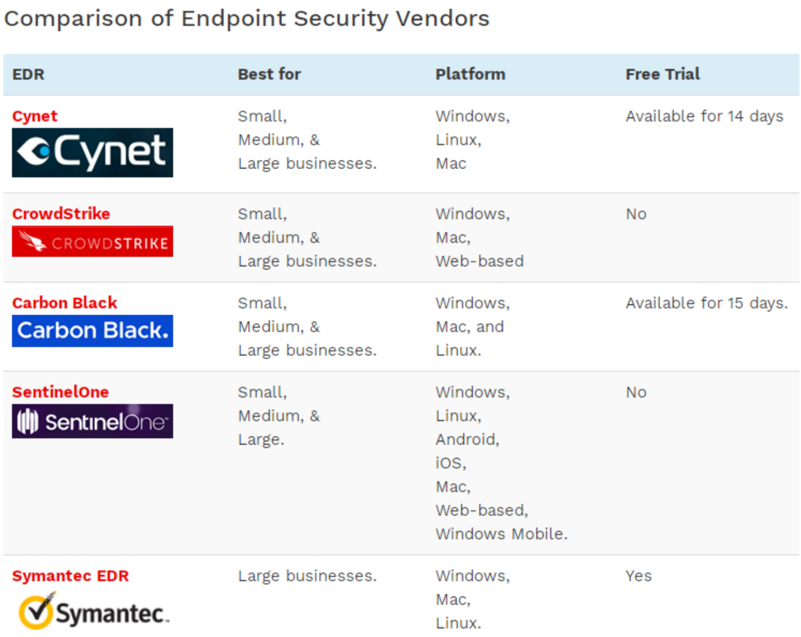
"Check Point Sandblast - The one and only Advanced Endpoint Protection (AEP)"

Check Point Sandblast Agent was for us the best suited Advanced Endpoint Protection. It was deployed quickly within our world-wide organization. The

Competitors and Alternatives

Check Point Software Technologies vs Palo Alto Networks
Check Point Software Technologies vs McAfee
Check Point Software Technologies vs Cisco

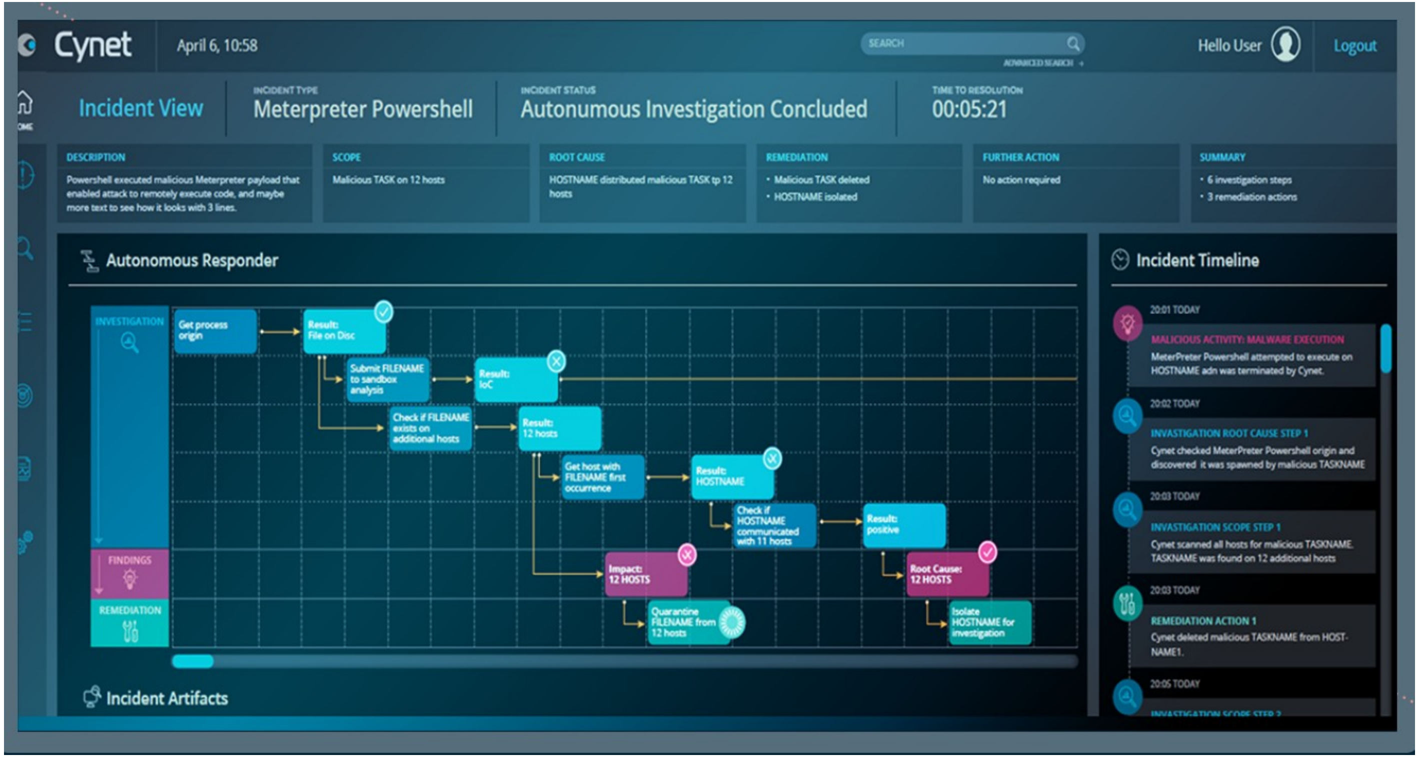
Aktuální produkty EndPoint Security softwaru



Comparison of Endpoint Security Vendors

EDR	Best for	Platform	Free Trial
Cynet	Small, Medium, & Large businesses.	Windows, Linux, Mac	Available for 14 days
CrowdStrike	Small, Medium, & Large businesses.	Windows, Mac, Web-based	No
Carbon Black	Small, Medium, & Large businesses.	Windows, Mac, and Linux.	Available for 15 days.
SentinelOne	Small, Medium, & Large.	Windows, Linux, Android, iOS, Mac, Web-based, Windows Mobile.	No
Symantec EDR	Large businesses.	Windows, Mac, Linux.	Yes

Cynet



Incident View

INCIDENT TYPE
Meterpreter Powershell

INCIDENT STATUS
Autonumous Investigation Concluded

TIME TO RESOLUTION
00:05:21

DESCRIPTION
Powershell executed malicious Meterpreter payload that enabled attack to remotely execute code, and maybe more text to see how it looks with 3 lines.

SCOPE
Malicious TASK on 12 hosts

ROOT CAUSE
HOSTNAME distributed malicious TASK tp 12 hosts

REMEDIATION
- Malicious TASK deleted
- HOSTNAME isolated

FURTHER ACTION
No action required

SUMMARY
- 6 investigation steps
- 3 remediation actions

Autonomous Responder

INVESTIGATION
FINDINGS
REMEDIATION
Get process origin
Result: File on Disc
Submit FILENAME to sandbox analysis
Result: IoC
Check if FILENAME exists on additional hosts
Result: 12 hosts
Get host with FILENAME first occurrence
Result: HOSTNAME
Check if HOSTNAME communicated with 11 hosts
Result: positive
Impact: 12 HOSTS
Root Cause: 12 HOSTS
Quarantine FILENAME from 12 hosts
Isolate HOSTNAME for investigation

Incident Artifacts

Incident Timeline

20:01 TODAY
MALICIOUS ACTIVITY: MALWARE EXECUTION
MeterPreter Powershell attempted to execute on HOSTNAME adn was terminated by Cynet.

20:02 TODAY
INVASTIGATION ROOT CAUSE STEP 1
Cynet checked MeterPreter Powershell origin and discovered it was spawned by malicious TASKNAME

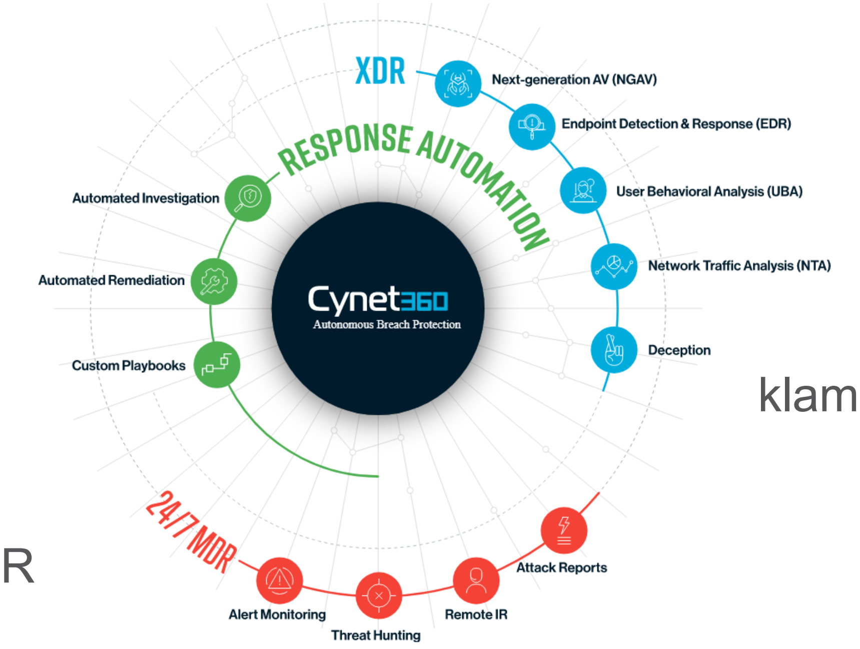
20:03 TODAY
INVASTIGATION SCOPE STEP 1
Cynet scanned all hosts for malicious TASKNAME. TASKNAME was found on 12 additional hosts

20:03 TODAY
REMEDIATION ACTION 1
Cynet deleted malicious TASKNAME from HOST-NAME1.

20:05 TODAY
INVASTIGATION SCOPE STEP 2

Přístup Cynetu

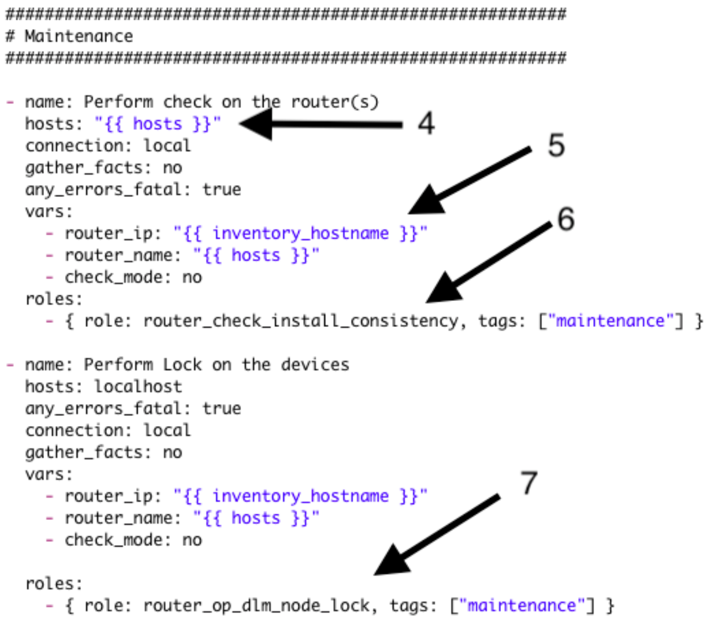
XDR Extension Detention and Response



klamání

Managed DR

Ukázka playbooku (Plays v YAML formátu)



```
##########################################################
# Maintenance
##########################################################

- name: Perform check on the router(s)
  hosts: "{{ hosts }}"
  connection: local
  gather_facts: no
  any_errors_fatal: true
  vars:
    - router_ip: "{{ inventory_hostname }}"
    - router_name: "{{ hosts }}"
    - check_mode: no
  roles:
    - { role: router_check_install_consistency, tags: ["maintenance"] }

- name: Perform Lock on the devices
  hosts: localhost
  any_errors_fatal: true
  connection: local
  gather_facts: no
  vars:
    - router_ip: "{{ inventory_hostname }}"
    - router_name: "{{ hosts }}"
    - check_mode: no

  roles:
    - { role: router_op_dlm_node_lock, tags: ["maintenance"] }
```

4	hosts	{{ hosts }}	This key is an Ansible magic variable. It is needed to identify the target device on which this Play will run. The value of this is a Jinja template, which Change Automation will substitute at runtime based on the devices selected by the user via the UI or API.
5	router_ip	{{ inventory_hostname }}	This key is a Cisco-defined variable needed for the Verb. The value is a Jinja template referencing an Ansible special variable.
6	role	router_check_install_consistency	This is another Cisco check Verb. See the Verb Reference for details.
7	role	router_op_dlm_node_lock	This is a Cisco action Verb. See the Verb Reference for details.

Cisco Email Security Appliance

The Cisco ESA device is designed to monitor Simple Mail Transfer Protocol (SMTP). The Cisco ESA is constantly updated by real-time feeds from the Cisco Talos, which detects and correlates threats and solutions by using a worldwide database monitoring system. This threat intelligence data is pulled by the Cisco ESA every three to five minutes.

These are some of the functions of the Cisco ESA:

- Block known threats
- Remediate against stealth malware that evaded initial detection
- Discard emails with bad links
- Block access to newly infected sites.
- Encrypt content in outgoing email to prevent data loss.

Cisco Web Security Appliance

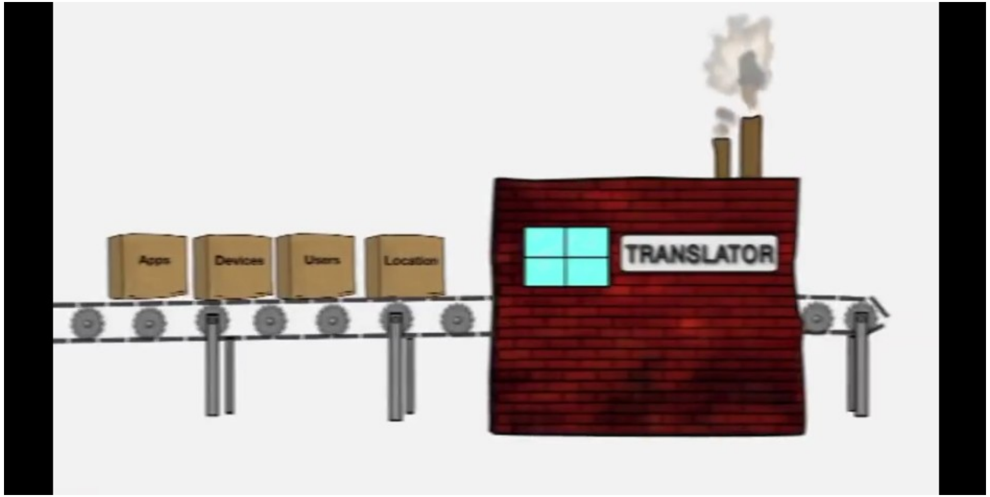
- The Cisco Web Security Appliance (WSA) is a mitigation technology for web-based threats. It helps organizations address the challenges of securing and controlling web traffic.
- The Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting.
- Cisco WSA provides complete control over how users access the internet. Certain features and applications, such as chat, messaging, video and audio, can be allowed, restricted with time and bandwidth limits, or blocked, according to the organization’s requirements.
- The WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, Web application filtering, and encryption and decryption of web traffic.

Vlastnosti Endpoint Security Softwaru

- Tradiční skenování koncových bodů a antivirové/antimalwarové funkce
- Plánované nebo nepřetržité sledování souborů a připojených zařízení
- Zamknutí či omezení přístupu ke koncovým bodům správcem
- Omezení přístupu k různým webům a aplikacím
- Integrovaný firewall
- Konfigurace a kontroly souladu se zásadami
- Automatizované aktualizace

Tools for Incident Prevention and Detection

- SIEM – Security Information and Event Management
  - Software that collects and analyzes security alerts, logs and other real time and historical data from security devices on the network
- DLP – Data Loss Prevention
  - Stops sensitive data from being stolen or escaped from the network
  - Designs to monitor and protect data in three different states
- Cisco Identity Services Engine (Cisco ISE) and TrustSec
  - Uses role-based access control policies

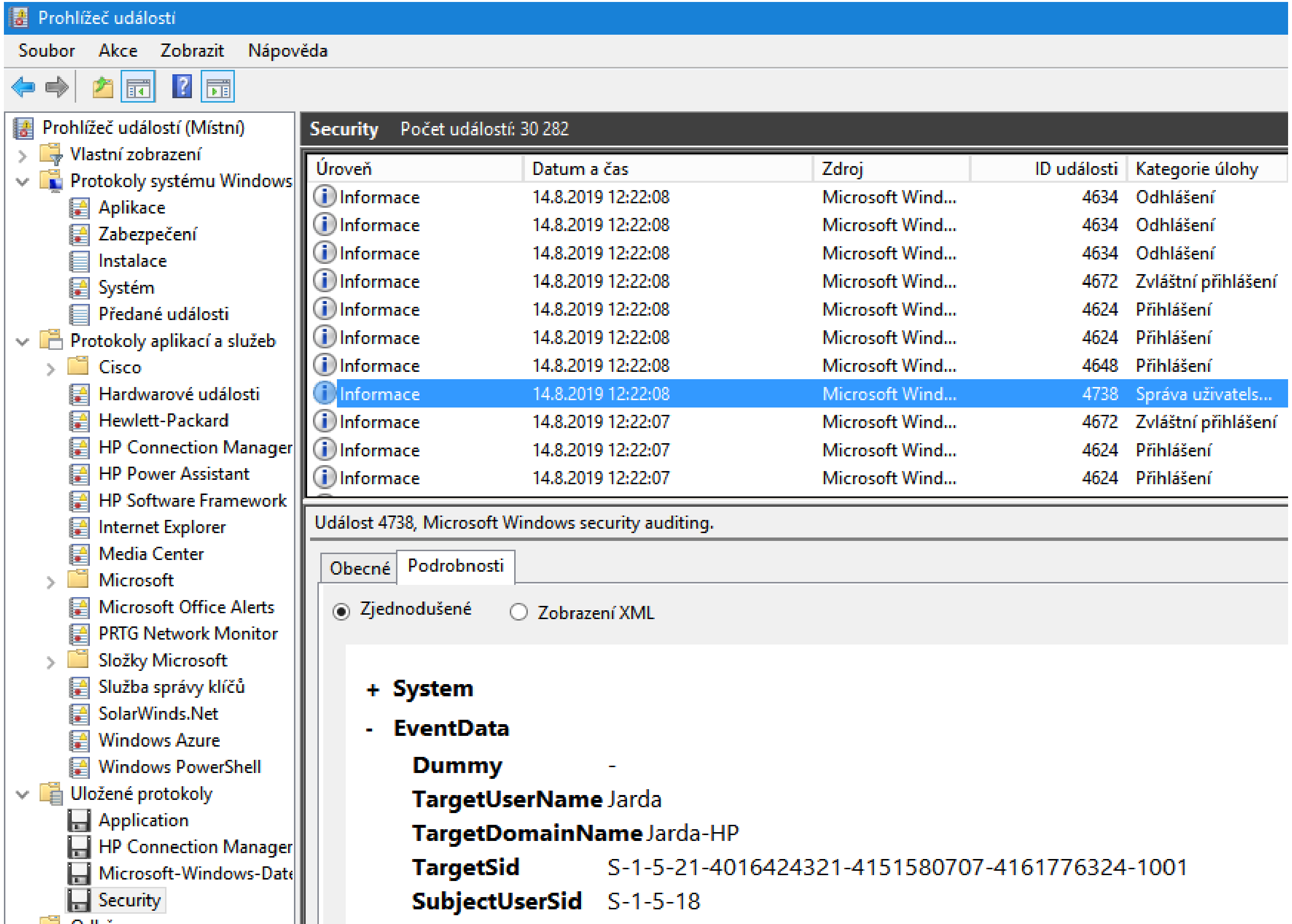


Architektura Cisco TrustSec

- kontrola přístupu založená na rolích
- všechny ověřovací mechanizmy se sbíhají do jediného centrálního systému: zjednodušuje správu bezpečnostních politik
- pomáhá udržovat integritu a diskrétnost dat po celou dobu jejich průchodu sítí: minimalizuje riziko úniku informací

Cisco ISE 3395 Identity Services Engine

Prohlížeč událostí na Windows



Security   Počet událostí: 30 282

Úroveň	Datum a čas	Zdroj	ID události	Kategorie úlohy
Informace	14.8.2019 12:22:08	Microsoft Wind...	4634	Odhlášení
Informace	14.8.2019 12:22:08	Microsoft Wind...	4634	Odhlášení
Informace	14.8.2019 12:22:08	Microsoft Wind...	4634	Odhlášení
Informace	14.8.2019 12:22:08	Microsoft Wind...	4672	Zvláštní přihlášení
Informace	14.8.2019 12:22:08	Microsoft Wind...	4624	Přihlášení
Informace	14.8.2019 12:22:08	Microsoft Wind...	4624	Přihlášení
Informace	14.8.2019 12:22:08	Microsoft Wind...	4648	Přihlášení
Informace	14.8.2019 12:22:08	Microsoft Wind...	4738	Správa uživatels...
Informace	14.8.2019 12:22:07	Microsoft Wind...	4672	Zvláštní přihlášení
Informace	14.8.2019 12:22:07	Microsoft Wind...	4624	Přihlášení
Informace	14.8.2019 12:22:07	Microsoft Wind...	4624	Přihlášení

Událost 4738, Microsoft Windows security auditing.

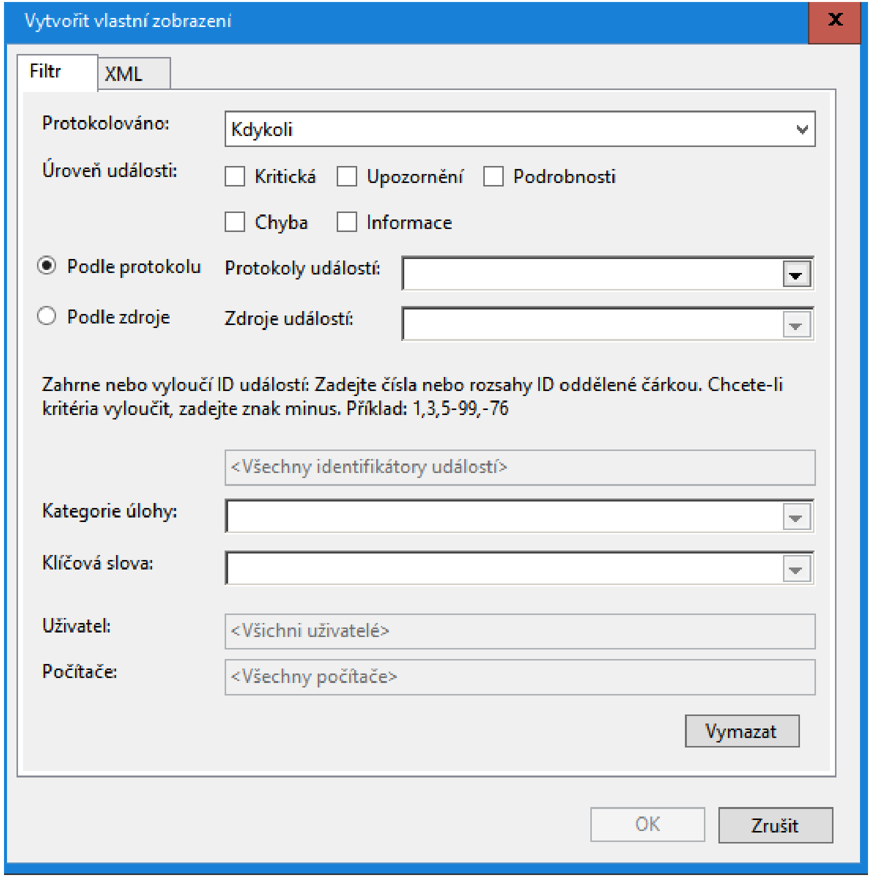
● Zjednodušené   ○ Zobrazení XML

+ System

- EventData

Dummy	-
TargetUserName	Jarda
TargetDomainName	Jarda-HP
TargetSid	S-1-5-21-4016424321-4151580707-4161776324-1001
SubjectUserSid	S-1-5-18

V prohlížeči událostí hledáme pomocí filtru



Protokolováno: Kdykoli

Úroveň události: □ Kritická □ Upozornění □ Podrobnosti □ Chyba □ Informace

● Podle protokolu Protokoly událostí:

○ Podle zdroje Zdroje událostí:

Zahrne nebo vyloučí ID událostí: Zadejte čísla nebo rozsahy ID oddělené čárkou. Chcete-li kritéria vyloučit, zadejte znak minus. Příklad: 1,3,5-99,-76

<Všechny identifikátory událostí>

Kategorie úlohy:

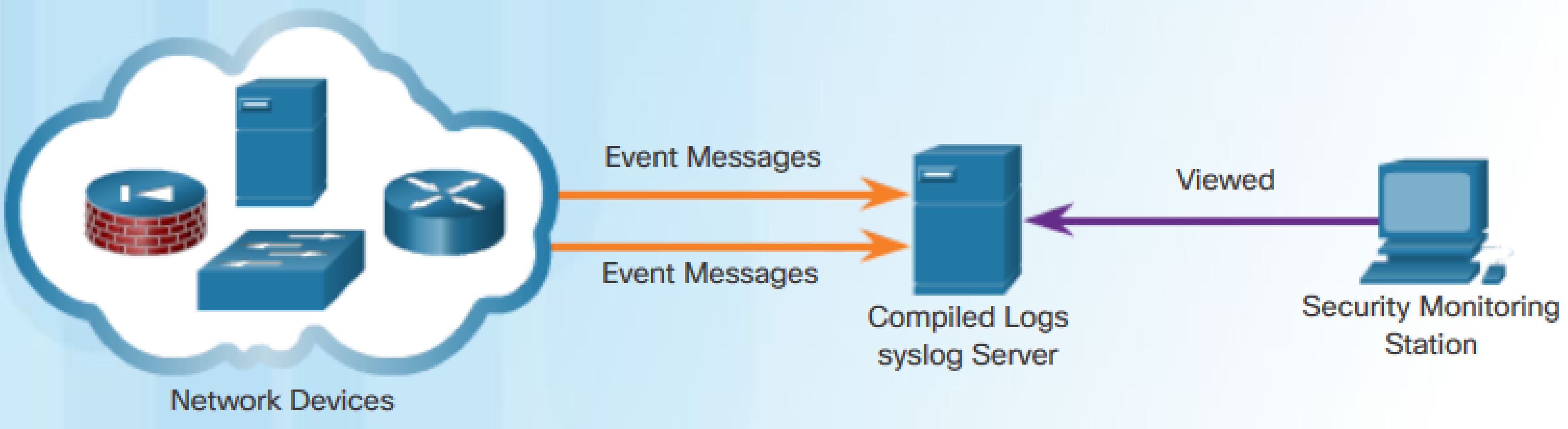
Klíčová slova:

Uživatel: <Všichni uživatelé>

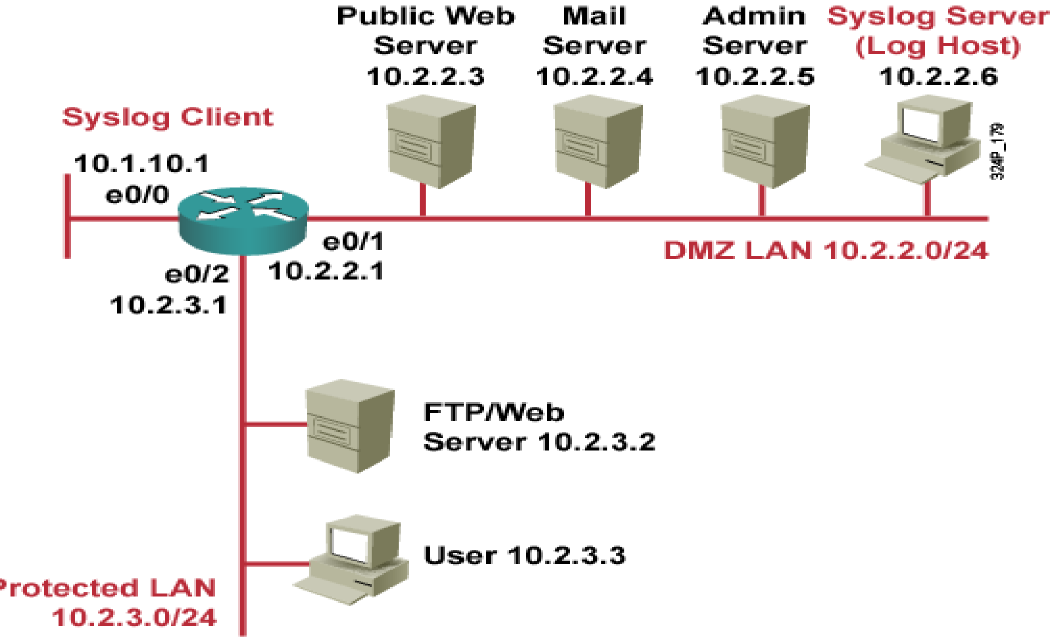
Počítače: <Všechny počítače>

Syslog server

- Slouží pro sběr logů ze síťových a koncových zařízení.
- Typicky naslouchá na UDP portu 514.
- Hackeři mohou blokovat přenos dat, manipulovat s daty protokolu nebo manipulovat se softwarem, který vytváří a přenáší zprávy protokolu.
- 1980 –> Syslog, 1998 –> Syslog-ng (podpora TLS a šifrování) , 2004 –> rsyslog (protokol RELP – Reliable Event Logging Protocol)



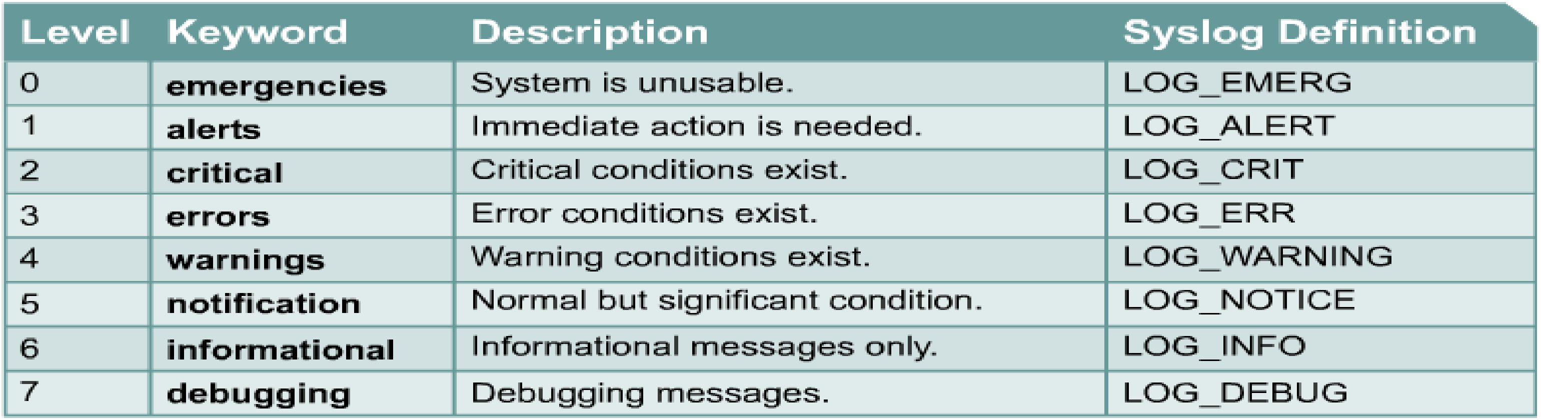
Do sítě doplníme syslog server



```
R3(config)# logging 10.2.2.6
R3(config)# logging trap informational
R3(config)# logging source-interface loopback 0
R3(config)# logging on
```

Úrovně chybových zpráv systému logování syslog

Nejvyšší úroveň

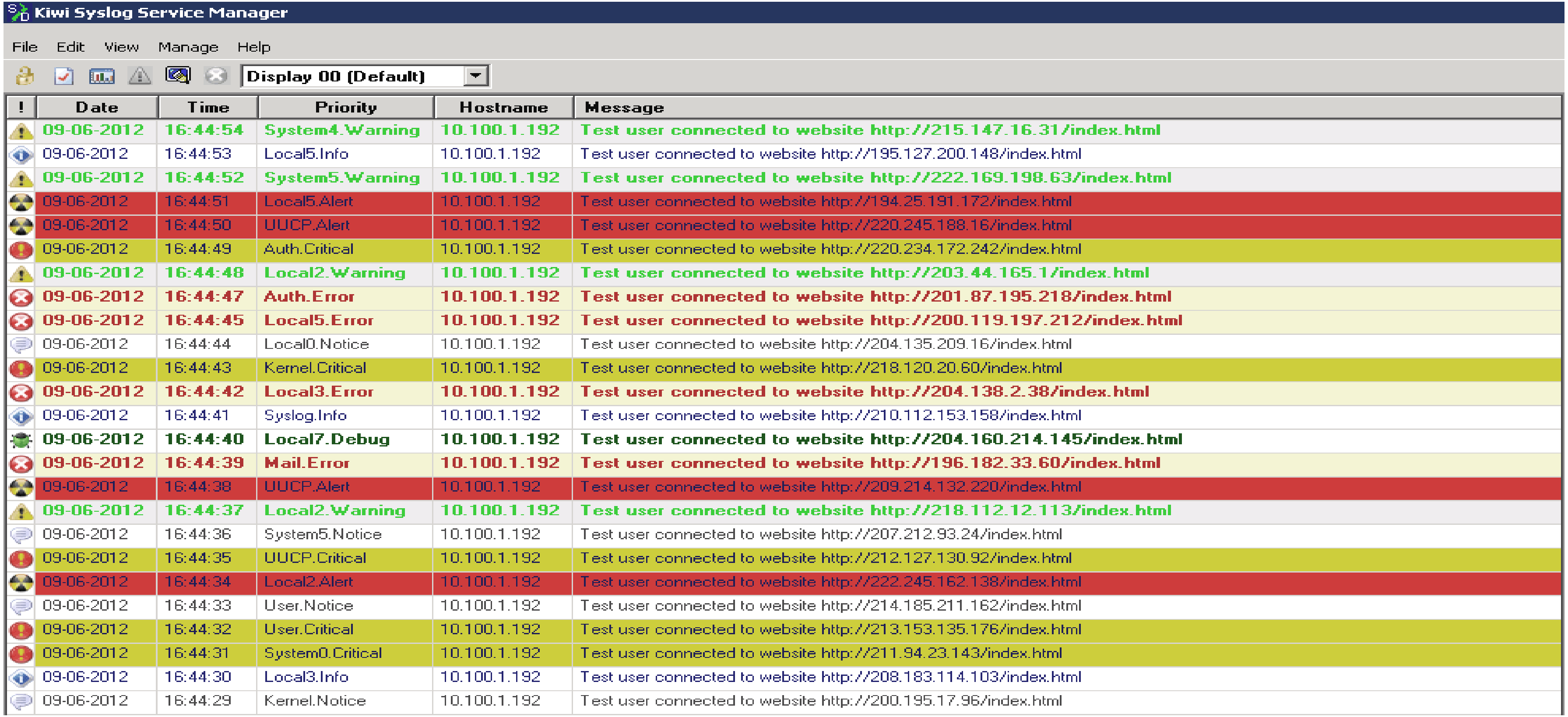


Level	Keyword	Description	Syslog Definition
0	**emergencies**	System is unusable.	LOG_EMERG
1	**alerts**	Immediate action is needed.	LOG_ALERT
2	**critical**	Critical conditions exist.	LOG_CRIT
3	**errors**	Error conditions exist.	LOG_ERR
4	**warnings**	Warning conditions exist.	LOG_WARNING
5	**notification**	Normal but significant condition.	LOG_NOTICE
6	**informational**	Informational messages only.	LOG_INFO
7	**debugging**	Debugging messages.	LOG_DEBUG

Nejnižší úroveň

Defaultní úroveň je 7 (debugging) – zprávy jsou posílány na konzolový port směrovače (line con0).

Dostaneme záplavu výstupů (zde Kiwi)

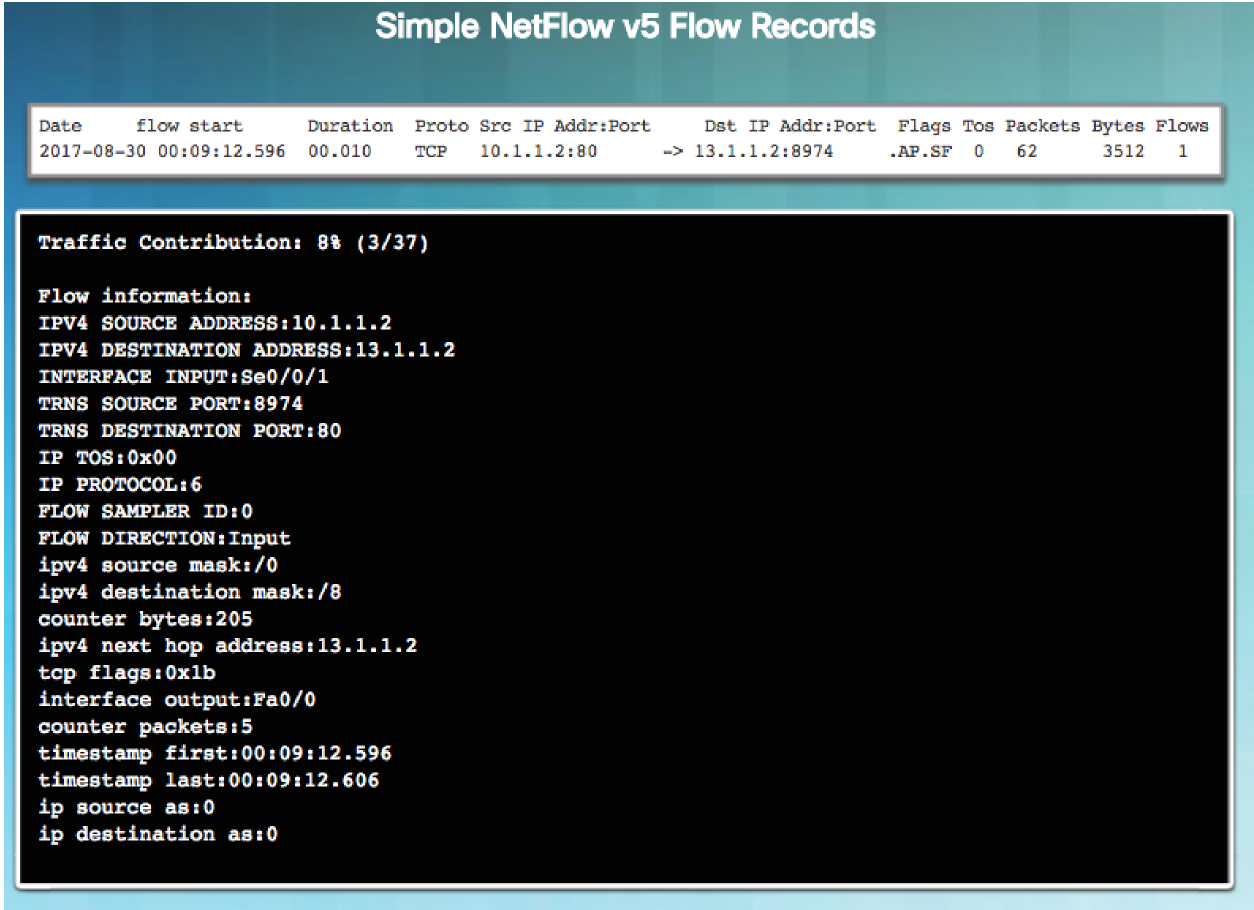


Display 00 (Default)

!	Date	Time	Priority	Hostname	Message
⚠	09-06-2012	16:44:54	System4.Warning	10.100.1.192	Test user connected to website http://215.147.16.31/index.html
ℹ	09-06-2012	16:44:53	Local5.Info	10.100.1.192	Test user connected to website http://195.127.200.148/index.html
⚠	09-06-2012	16:44:52	System5.Warning	10.100.1.192	Test user connected to website http://222.169.198.63/index.html
☢	09-06-2012	16:44:51	Local5.Alert	10.100.1.192	Test user connected to website http://194.25.191.172/index.html
☢	09-06-2012	16:44:50	UUCP.Alert	10.100.1.192	Test user connected to website http://220.245.188.16/index.html
❗	09-06-2012	16:44:49	Auth.Critical	10.100.1.192	Test user connected to website http://220.234.172.242/index.html
⚠	09-06-2012	16:44:48	Local2.Warning	10.100.1.192	Test user connected to website http://203.44.165.1/index.html
⊗	09-06-2012	16:44:47	Auth.Error	10.100.1.192	Test user connected to website http://201.87.195.218/index.html
⊗	09-06-2012	16:44:45	Local5.Error	10.100.1.192	Test user connected to website http://200.119.197.212/index.html
💬	09-06-2012	16:44:44	Local0.Notice	10.100.1.192	Test user connected to website http://204.135.209.16/index.html
❗	09-06-2012	16:44:43	Kernel.Critical	10.100.1.192	Test user connected to website http://218.120.20.60/index.html
⊗	09-06-2012	16:44:42	Local3.Error	10.100.1.192	Test user connected to website http://204.138.2.38/index.html
ℹ	09-06-2012	16:44:41	Syslog.Info	10.100.1.192	Test user connected to website http://210.112.153.158/index.html
🐞	09-06-2012	16:44:40	Local7.Debug	10.100.1.192	Test user connected to website http://204.160.214.145/index.html
⊗	09-06-2012	16:44:39	Mail.Error	10.100.1.192	Test user connected to website http://196.182.33.60/index.html
☢	09-06-2012	16:44:38	UUCP.Alert	10.100.1.192	Test user connected to website http://209.214.132.220/index.html
⚠	09-06-2012	16:44:37	Local2.Warning	10.100.1.192	Test user connected to website http://218.112.12.113/index.html
💬	09-06-2012	16:44:36	System5.Notice	10.100.1.192	Test user connected to website http://207.212.93.24/index.html
❗	09-06-2012	16:44:35	UUCP.Critical	10.100.1.192	Test user connected to website http://212.127.130.92/index.html
☢	09-06-2012	16:44:34	Local2.Alert	10.100.1.192	Test user connected to website http://222.245.162.138/index.html
💬	09-06-2012	16:44:33	User.Notice	10.100.1.192	Test user connected to website http://214.185.211.162/index.html
❗	09-06-2012	16:44:32	User.Critical	10.100.1.192	Test user connected to website http://213.153.135.176/index.html
❗	09-06-2012	16:44:31	System0.Critical	10.100.1.192	Test user connected to website http://211.94.23.143/index.html
ℹ	09-06-2012	16:44:30	Local3.Info	10.100.1.192	Test user connected to website http://208.183.114.103/index.html
💬	09-06-2012	16:44:29	Kernel.Notice	10.100.1.192	Test user connected to website http://200.195.17.96/index.html

NetFlow

- Umožňuje účtování síťového provozu, plánování sítě, zabezpečení, možnosti sledování odmítnutí služby a monitorování sítě.
- Poskytuje informace o uživatelích a aplikacích sítě, dobách využití špiček a směrování provozu.
- **Shromažďuje metadata** nebo data o toku, nikoli samotná data toku.

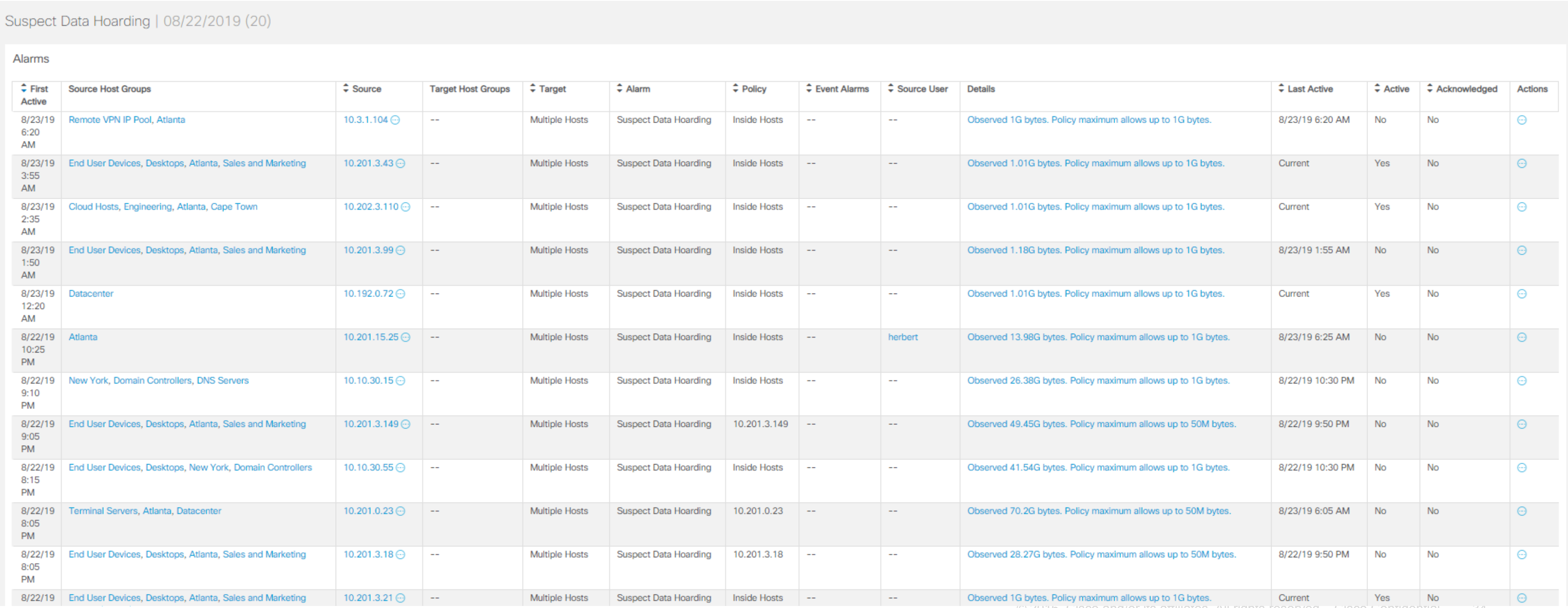


Simple NetFlow v5 Flow Records

```
Date       flow start        Duration  Proto Src IP Addr:Port      Dst IP Addr:Port   Flags Tos Packets Bytes Flows
2017-08-30 00:09:12.596      00.010    TCP   10.1.1.2:80        -> 13.1.1.2:8974     .AP.SF  0    62      3512   1
```

```
Traffic Contribution: 8% (3/37)

Flow information:
IPV4 SOURCE ADDRESS:10.1.1.2
IPV4 DESTINATION ADDRESS:13.1.1.2
INTERFACE INPUT:Se0/0/1
TRNS SOURCE PORT:8974
TRNS DESTINATION PORT:80
IP TOS:0x00
IP PROTOCOL:6
FLOW SAMPLER ID:0
FLOW DIRECTION:Input
ipv4 source mask:/0
ipv4 destination mask:/8
counter bytes:205
ipv4 next hop address:13.1.1.2
tcp flags:0x1b
interface output:Fa0/0
counter packets:5
timestamp first:00:09:12.596
timestamp last:00:09:12.606
ip source as:0
ip destination as:0
```

Sledování toků ve Stealwatch



Suspect Data Hoarding | 08/22/2019 (20)

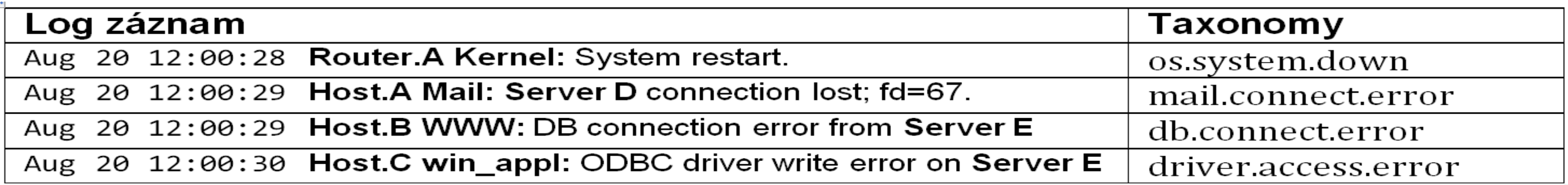
Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Event Alarms	Source User	Details	Last Active	Active	Acknowledged	Actions
8/23/19 6:20 AM	Remote VPN IP Pool, Atlanta	10.3.1.104	--	Multiple Hosts	Suspect Data Hoarding	Inside Hosts	--	--	Observed 1G bytes. Policy maximum allows up to 1G bytes.	8/23/19 6:20 AM	No	No	⊖
8/23/19 3:55 AM	End User Devices, Desktops, Atlanta, Sales and Marketing	10.201.3.43	--	Multiple Hosts	Suspect Data Hoarding	Inside Hosts	--	--	Observed 1.01G bytes. Policy maximum allows up to 1G bytes.	Current	Yes	No	⊖
8/23/19 2:35 AM	Cloud Hosts, Engineering, Atlanta, Cape Town	10.202.3.110	--	Multiple Hosts	Suspect Data Hoarding	Inside Hosts	--	--	Observed 1.01G bytes. Policy maximum allows up to 1G bytes.	Current	Yes	No	⊖
8/23/19 1:50 AM	End User Devices, Desktops, Atlanta, Sales and Marketing	10.201.3.99	--	Multiple Hosts	Suspect Data Hoarding	Inside Hosts	--	--	Observed 1.18G bytes. Policy maximum allows up to 1G bytes.	8/23/19 1:55 AM	No	No	⊖
8/23/19 12:20 AM	Datacenter	10.192.0.72	--	Multiple Hosts	Suspect Data Hoarding	Inside Hosts	--	--	Observed 1.01G bytes. Policy maximum allows up to 1G bytes.	Current	Yes	No	⊖
8/22/19 10:25 PM	Atlanta	10.201.15.25	--	Multiple Hosts	Suspect Data Hoarding	Inside Hosts	--	herbert	Observed 13.98G bytes. Policy maximum allows up to 1G bytes.	8/23/19 6:25 AM	No	No	⊖
8/22/19 9:10 PM	New York, Domain Controllers, DNS Servers	10.10.30.15	--	Multiple Hosts	Suspect Data Hoarding	Inside Hosts	--	--	Observed 26.38G bytes. Policy maximum allows up to 1G bytes.	8/22/19 10:30 PM	No	No	⊖
8/22/19 9:05 PM	End User Devices, Desktops, Atlanta, Sales and Marketing	10.201.3.149	--	Multiple Hosts	Suspect Data Hoarding	10.201.3.149	--	--	Observed 49.45G bytes. Policy maximum allows up to 50M bytes.	8/22/19 9:50 PM	No	No	⊖
8/22/19 8:15 PM	End User Devices, Desktops, New York, Domain Controllers	10.10.30.55	--	Multiple Hosts	Suspect Data Hoarding	Inside Hosts	--	--	Observed 41.54G bytes. Policy maximum allows up to 1G bytes.	8/22/19 10:30 PM	No	No	⊖
8/22/19 8:05 PM	Terminal Servers, Atlanta, Datacenter	10.201.0.23	--	Multiple Hosts	Suspect Data Hoarding	10.201.0.23	--	--	Observed 70.2G bytes. Policy maximum allows up to 50M bytes.	8/23/19 6:05 AM	No	No	⊖
8/22/19 8:05 PM	End User Devices, Desktops, Atlanta, Sales and Marketing	10.201.3.18	--	Multiple Hosts	Suspect Data Hoarding	10.201.3.18	--	--	Observed 28.27G bytes. Policy maximum allows up to 50M bytes.	8/22/19 9:50 PM	No	No	⊖
8/22/19	End User Devices, Desktops, Atlanta, Sales and Marketing	10.201.3.21	--	Multiple Hosts	Suspect Data Hoarding	Inside Hosts	--	--	Observed 1G bytes. Policy maximum allows up to 1G bytes.	Current	Yes	No	⊖

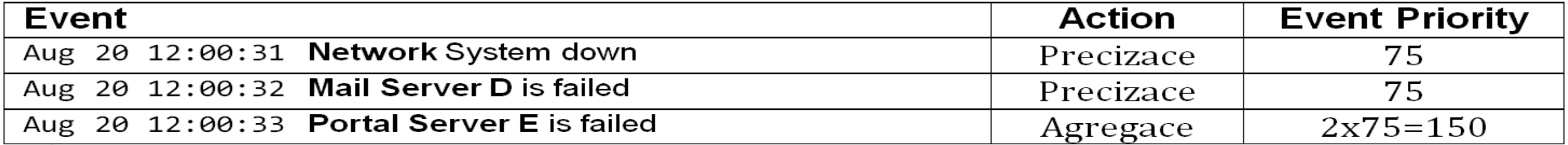
ELK umí log management, ale ne korelační funkce atd.

- Elastic Search – distribuovaný vyhledávací engine
- Logstash – nástroj pro směrování zpráv
- Kibana – HTML rozhraní pro zobrazování dat z Elastic Search

SIEM: Zápisu logů je převeden do zápisu událostí



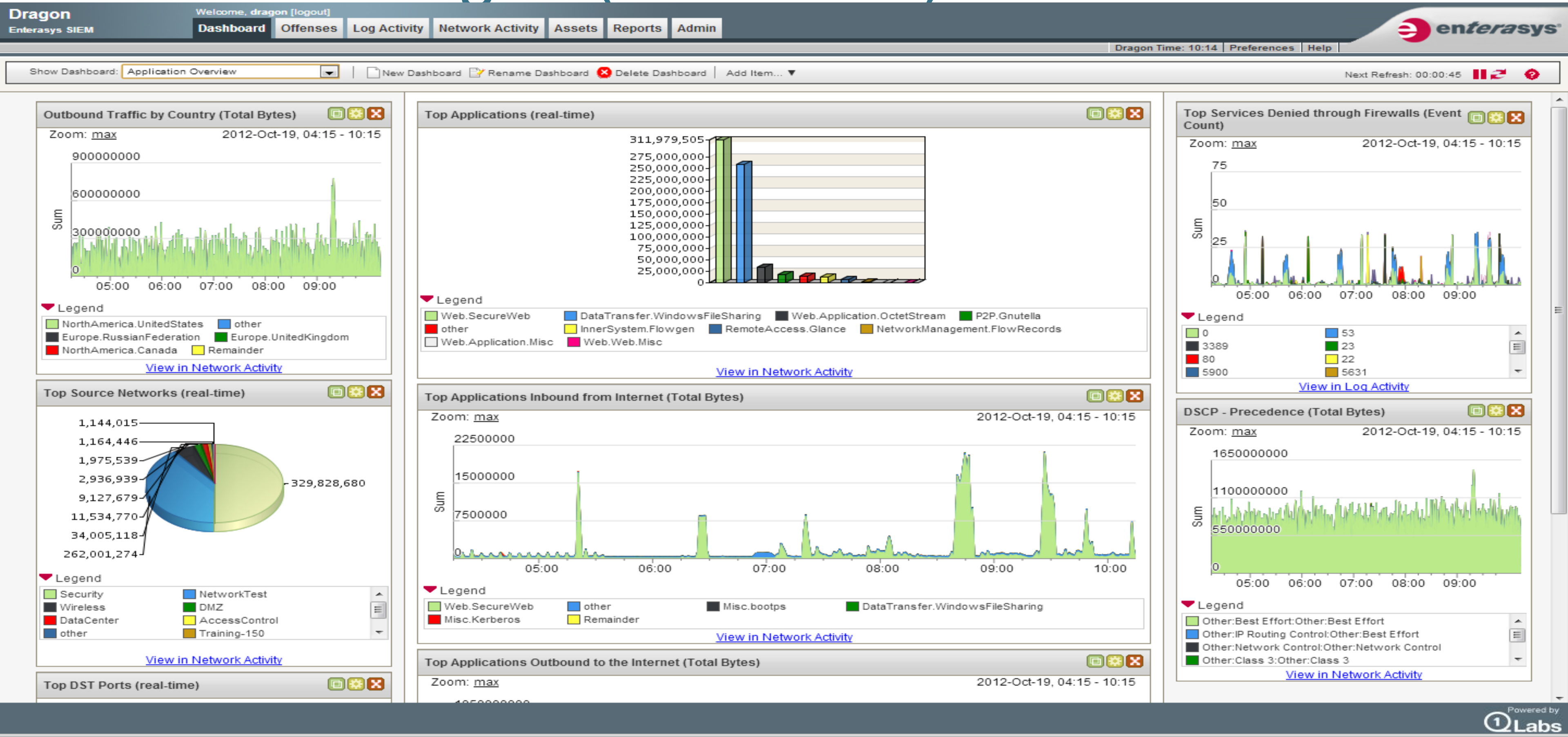
Log záznam	Taxonomy
Aug 20 12:00:28 **Router.A Kernel:** System restart.	os.system.down
Aug 20 12:00:29 **Host.A Mail: Server D** connection lost; fd=67.	mail.connect.error
Aug 20 12:00:29 **Host.B WWW:** DB connection error from **Server E**	db.connect.error
Aug 20 12:00:30 **Host.C win_appl:** ODBC driver write error on **Server E**	driver.access.error



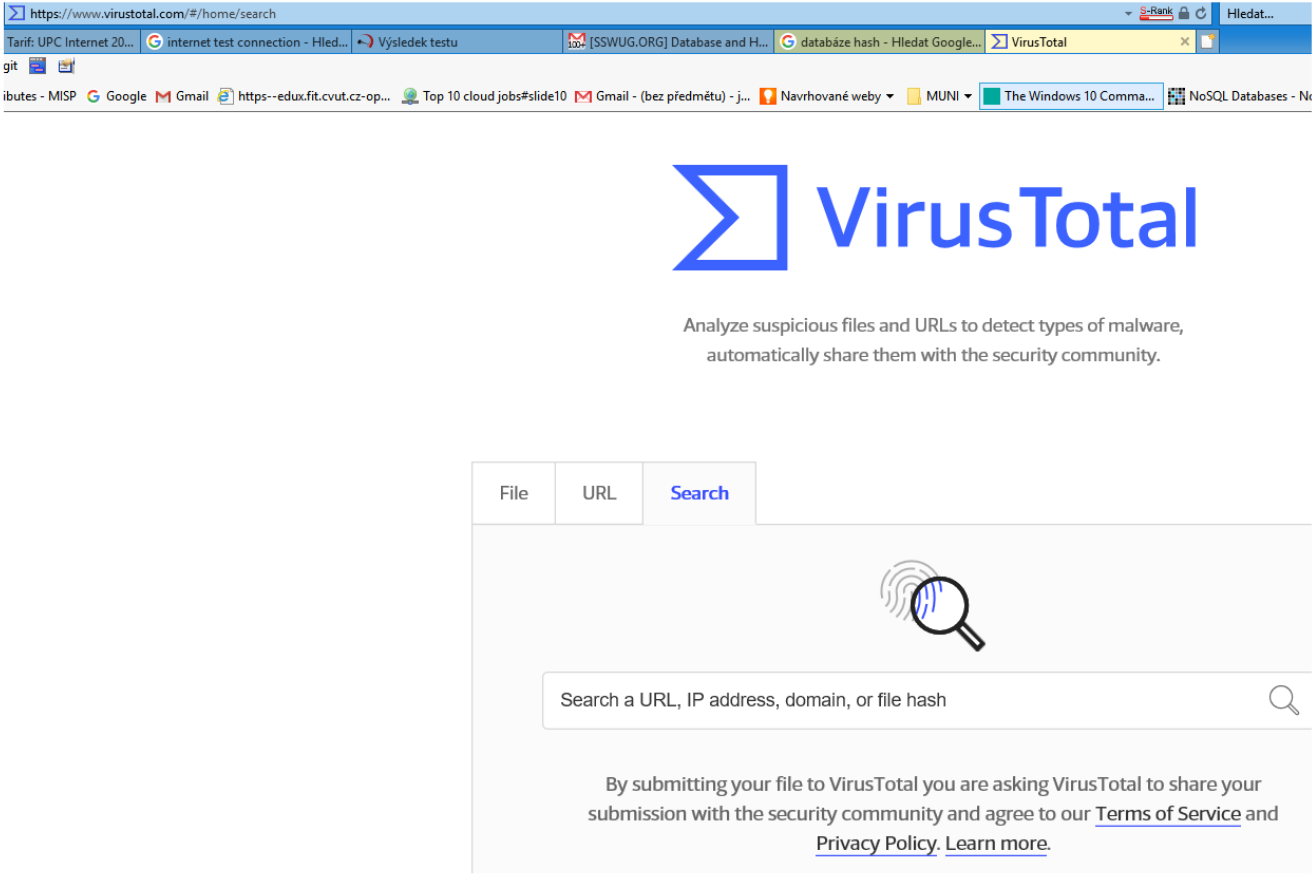
Event	Action	Event Priority
Aug 20 12:00:31 **Network** System down	Precizace	75
Aug 20 12:00:32 **Mail Server D** is failed	Precizace	75
Aug 20 12:00:33 **Portal Server E** is failed	Agregace	2x75=150

- **Precizace** probíhají pomocí substitucí: Router.A=Network, Host.A=Mail, Host.B/Host.C=Portal. a přidáním bezpečnostní hodnoty události (Event Priority).
- **Agregace** může být v SIEM volitelně provedena nejen nad událostmi, ale i nad „vytěženou informací“, jako např. na *source_hostname*, *source_ip*, *target_hostname*, *target_ip*, atp.
- **Korelace** je pokročilejší agregace, neboť pracuje z různými formáty událostí mající stejnou kategorii děje = taxonomy.

Příklad: Dragon (OEM IBM) - dashboard



Virus Total



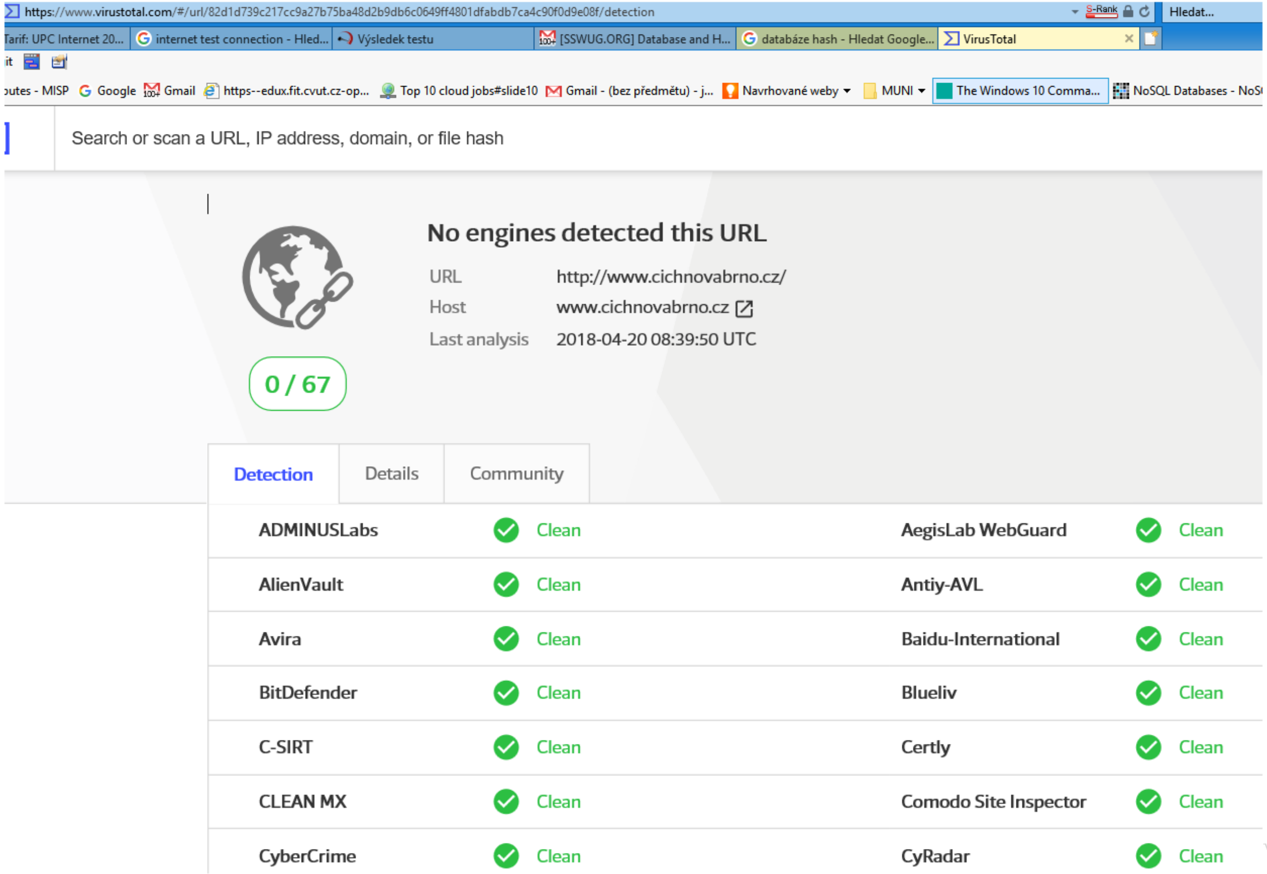
https://www.virustotal.com/#/home/search
S-Rank
Hledat...
Tarif: UPC Internet 20...
internet test connection - Hled...
Výsledek testu
[SSWUG.ORG] Database and H...
databáze hash - Hledat Google...
VirusTotal
git
ibutes - MISP
Google
Gmail
https--edux.fit.cvut.cz-op...
Top 10 cloud jobs#slide10
Gmail - (bez předmětu) - j...
Navrhované weby
MUNI
The Windows 10 Comma...
NoSQL Databases - N
VirusTotal
File
URL
Search

Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.

Search a URL, IP address, domain, or file hash

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our Terms of Service and Privacy Policy. Learn more.

Virus Total výsledek


https://www.virustotal.com/#/url/82d1d739c217cc9a27b75ba48d2b9db6c0649ff4801dfabdb7ca4c90f0d9e08f/detection
S-Rank
Hledat...
Tarif: UPC Internet 20...
internet test connection - Hled...
Výsledek testu
[SSWUG.ORG] Database and H...
databáze hash - Hledat Google...
VirusTotal
utes - MISP
Google
Gmail
https--edux.fit.cvut.cz-op...
Top 10 cloud jobs#slide10
Gmail - (bez předmětu) - j...
Navrhované weby
MUNI
The Windows 10 Comma...
NoSQL Databases - NoS
Search or scan a URL, IP address, domain, or file hash
Detection
Details
Community

No engines detected this URL

URL http://www.cichnovabrno.cz/

Host www.cichnovabrno.cz

Last analysis 2018-04-20 08:39:50 UTC

0 / 67

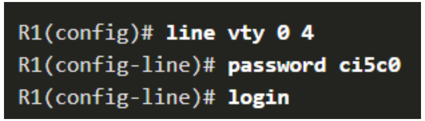
ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AlienVault	Clean	Antiy-AVL	Clean
Avira	Clean	Baidu-International	Clean
BitDefender	Clean	Blueliv	Clean
C-SIRT	Clean	Certly	Clean
CLEAN MX	Clean	Comodo Site Inspector	Clean
CyberCrime	Clean	CyRadar	Clean

10.2 Access Control

Authentication with a Local Password

Many types of authentication can be performed on networking devices, and each method offers varying levels of security.

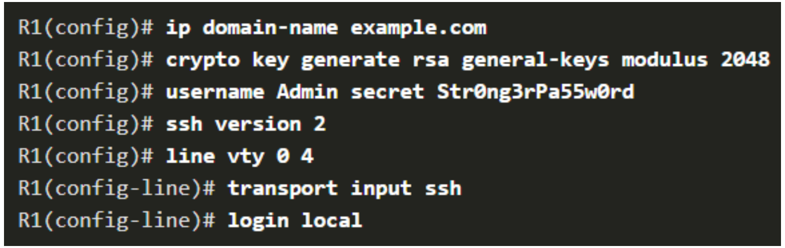
The simplest method of remote access authentication is to configure a login and password combination on console, vty lines, and aux ports.



```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

SSH is a more secure form of remote access:

- It requires a username and a password.
- The username and password can be authenticated locally.



```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

The local database method has some limitations:

- User accounts must be configured locally on each device which is not scalable.
- The method provides no fallback authentication method.

AAA Components

AAA stands for Authentication, Authorization, and Accounting, and provides the primary framework to set up access control on a network device.

AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting).

Authentication

Local and server-based are two common methods of implementing AAA authentication.

Local AAA Authentication:

- Method stores usernames and passwords locally in a network device (e.g., Cisco router).
- Users authenticate against the local database.
- Local AAA is ideal for small networks.

Server-Based AAA Authentication:

- With the server-based method, the router accesses a central AAA server.
- The AAA server contains the usernames and password for all users.
- The router uses either the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) protocols to communicate with the AAA server.
- When there are multiple routers and switches, server-based AAA is more appropriate.

Authorization

- AAA authorization is automatic and does not require users to perform additional steps after authentication.

- Authorization governs what users can and cannot do on the network after they are authenticated.

- Authorization uses a set of attributes that describes the user’s access to the network. These attributes are used by the AAA server to determine privileges and restrictions for that user.

Accounting

AAA accounting collects and reports usage data. This data can be used for such purposes as auditing or billing. The collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes.

A primary use of accounting is to combine it with AAA authentication.

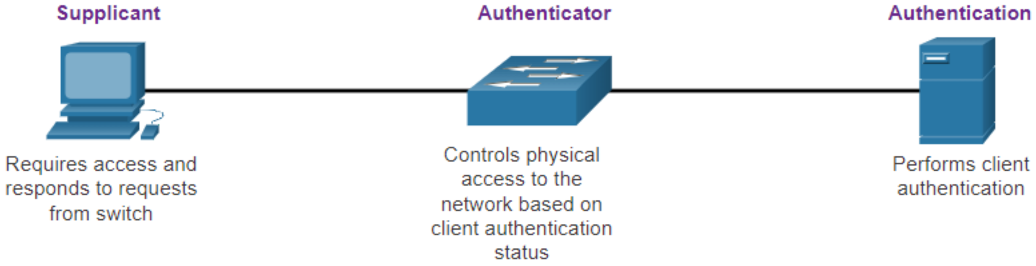
- The AAA server keeps a detailed log of exactly what the authenticated user does on the device, as shown in the figure. This includes all EXEC and configuration commands issued by the user.
- The log contains numerous data fields, including the username, the date and time, and the actual command that was entered by the user. This information is useful when troubleshooting devices. It also provides evidence for when individuals perform malicious acts.

802.1X

The IEEE 802.1X standard is a port-based access control and authentication protocol. This protocol restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports. The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN.

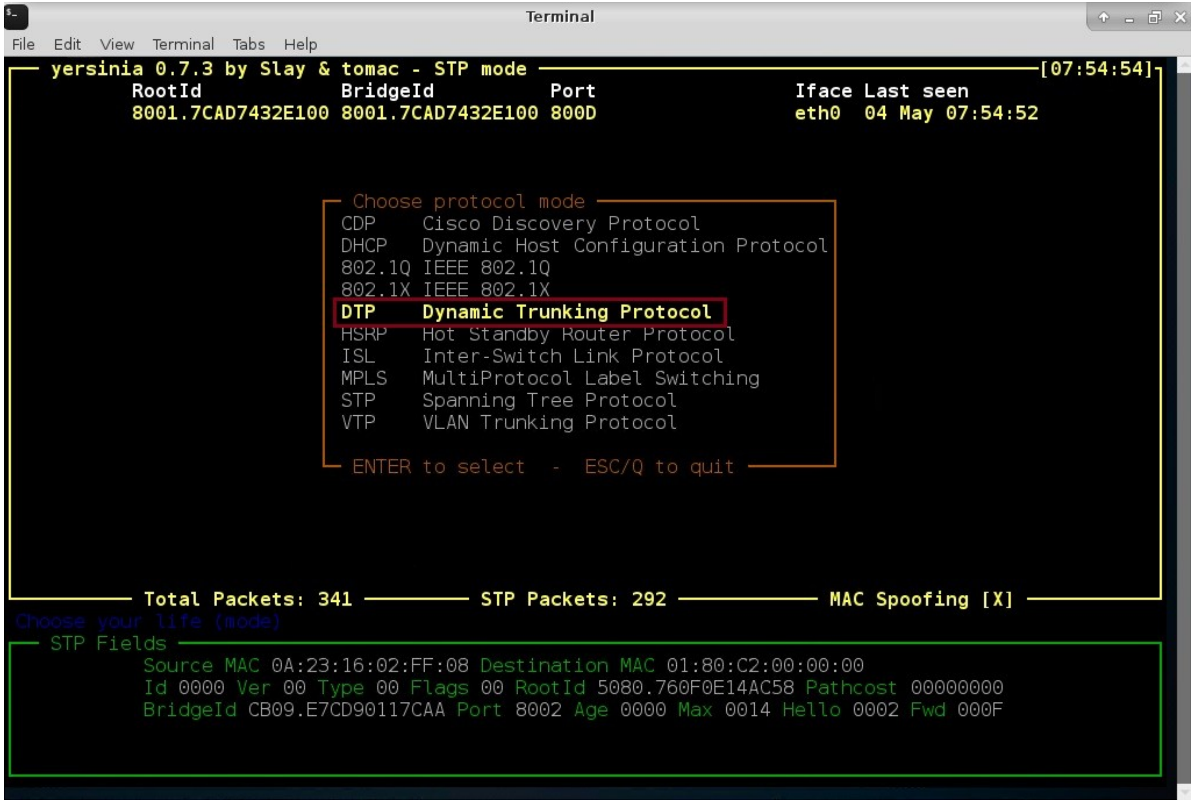
With 802.1X port-based authentication, the devices in the network have specific roles:

- **Client (Supplicant)** - This is a device running 802.1X-compliant client software, which is available for wired or wireless devices.
- **Switch (Authenticator)** –The switch acts as an intermediary between the client and the authentication server. It requests identifying information from the client, verifies that information with the authentication server, and relays a response to the client. Another device that could act as authenticator is a wireless access point.
- **Authentication server** –The server validates the identity of the client and notifies the switch or wireless access point that the client is or is not authorized to access the LAN and switch services.


Supplicant
Authenticator
Authentication
Requires access and responds to requests from switch
Controls physical access to the network based on client authentication status
Performs client authentication

Konkrétní útok pomocí yersinie

http://www.jay-miah.co.uk/vlan-hopping-concept-attack-example-and-prevention/



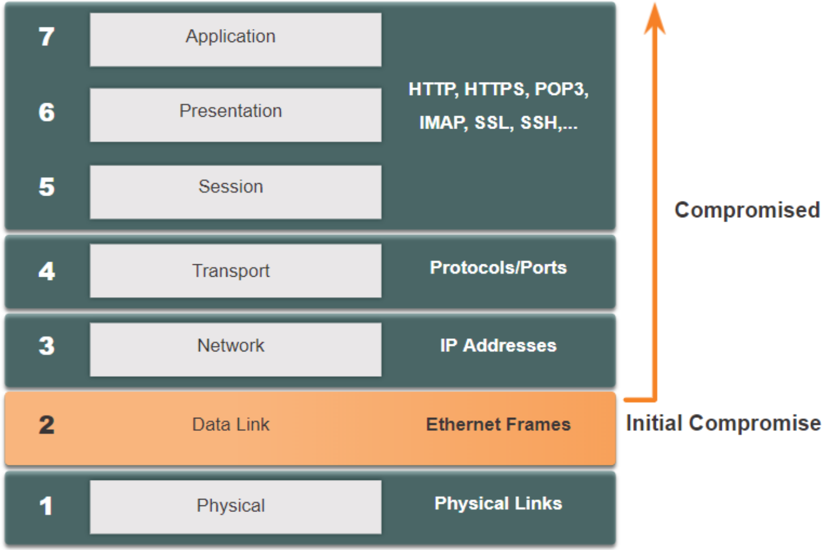
```
 yersinia 0.7.3 by Slay & tomac - STP mode ---------------------------------[07:54:54]
           RootId           BridgeId          Port                 Iface Last seen
           8001.7CAD7432E100 8001.7CAD7432E100 800D                 eth0  04 May 07:54:52



                           Choose protocol mode
                          CDP    Cisco Discovery Protocol
                          DHCP   Dynamic Host Configuration Protocol
                          802.1Q IEEE 802.1Q
                          802.1X IEEE 802.1X
                          DTP    Dynamic Trunking Protocol
                          HSRP   Hot Standby Router Protocol
                          ISL    Inter-Switch Link Protocol
                          MPLS   MultiProtocol Label Switching
                          STP    Spanning Tree Protocol
                          VTP    VLAN Trunking Protocol

                           ENTER to select  -  ESC/Q to quit




            Total Packets: 341 ------- STP Packets: 292 ---------- MAC Spoofing [X]
Choose your life (mode)
 STP Fields
            Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00
            Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 00000000
            BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
```

10.3 Layer 2 Security Threats

Layer 2 Vulnerabilities

Recall that the OSI reference model is divided into seven layers which work independently of each other. The figure shows the function of each layer and the core elements that can be exploited.

Network administrators routinely implement security solutions to protect the elements in Layer 3 up through Layer 7. They use VPNs, firewalls, and IPS devices to protect these elements. However, if Layer 2 is compromised, then all the layers above it are also affected. For example, if a threat actor with access to the internal network captured Layer 2 frames, then all the security implemented on the layers above would be useless. The threat actor could cause a lot of damage on the Layer 2 LAN networking infrastructure.



Switch Attack Categories

Security is only as strong as the weakest link in the system, and Layer 2 is considered to be that weak link. This is because LANs were traditionally under the administrative control of a single organization. We inherently trusted all persons and devices connected to our LAN. Today, with BYOD and more sophisticated attacks, our LANs have become more vulnerable to penetration.

Category	Examples
MAC Table Attacks	Includes MAC address flooding attacks.
VLAN Attacks	Includes VLAN hopping and VLAN double-tagging attacks. It also includes attacks between devices on a common VLAN.
DHCP Attacks	Includes DHCP starvation and DHCP spoofing attacks.
ARP Attacks	Includes ARP spoofing and ARP poisoning attacks.
Address Spoofing Attacks	Includes MAC address and IP address spoofing attacks.
STP Attacks	Includes Spanning Tree Protocol manipulation attacks.

arpspoof v Kali

1. Kontrola defaultní brány: ip route
2. Oskenování sítě: netdiscover -r 192.168.1.0/24 -r … range

3. Útok: arpspoof -i `eth0` -t *`192.168.1.10`* -r *`192.168.1.1`*

arp skener ve scapy

```
from scapy.all import *def arp_scan(ip):

      request = Ether(dst="ff:ff:ff:ff:ff:ff") / ARP(pdst=ip)  ans, unans =
  srp(request, timeout=2, retry=1)
      result = []    for sent, received in ans:
          result.append({'IP': received.psrc, 'MAC': received.hwsrc})
  return result
```

Switch Attack Mitigation Techniques

Solution	Description
Port Security	Prevents many types of attacks including MAC address flooding attacks and DHCP starvation attacks.
DHCP Snooping	Prevents DHCP starvation and DHCP spoofing attacks.
Dynamic ARP Inspection (DAI)	Prevents ARP spoofing and ARP poisoning attacks.
IP Source Guard (IPSG)	Prevents MAC and IP address spoofing attacks.

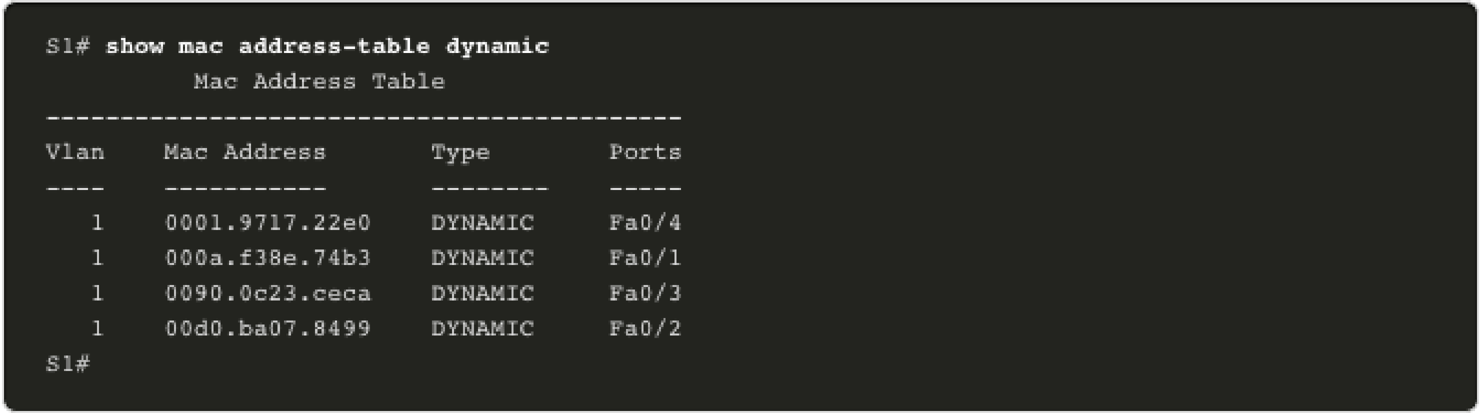
These Layer 2 solutions will not be effective if the management protocols are not secured. The following strategies are recommended:

- Always use secure variants of management protocols such as SSH, Secure Copy Protocol (SCP), Secure FTP (SFTP), and Secure Socket Layer/Transport Layer Security (SSL/TLS).
- Consider using out-of-band management network to manage devices.
- Use a dedicated management VLAN where nothing but management traffic resides.
- Use ACLs to filter unwanted access.

10.4 MAC Address Table Attack

Switch Operation Review

Recall that to make forwarding decisions, a Layer 2 LAN switch builds a table based on the source MAC addresses in received frames. This is called a MAC address table. MAC address tables are stored in memory and are used to more efficiently switch frames.



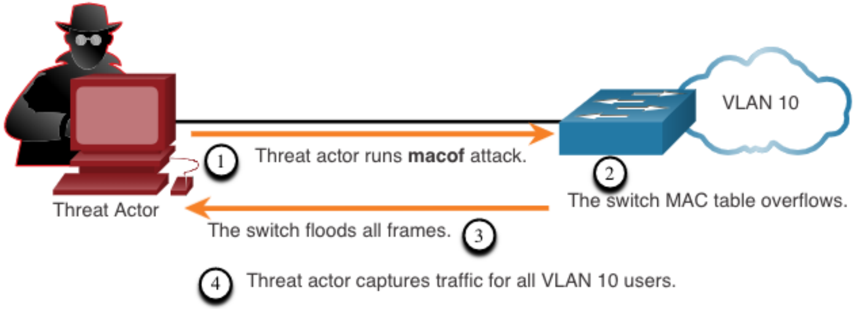
```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

MAC Address Table Flooding

All MAC tables have a fixed size and consequently, a switch can run out of resources in which to store MAC addresses. MAC address flooding attacks take advantage of this limitation by bombarding the switch with fake source MAC addresses until the switch MAC address table is full.

When this occurs, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic out all ports on the same VLAN without referencing the MAC table. This condition now allows a threat actor to capture all of the frames sent from one host to another on the local LAN or local VLAN.

Note: Traffic is flooded only within the local LAN or VLAN. The threat actor can only capture traffic within the local LAN or VLAN to which the threat actor is connected.


Threat Actor
VLAN 10
1 Threat actor runs **macof** attack.
2 The switch MAC table overflows.
The switch floods all frames. 3
4 Threat actor captures traffic for all VLAN 10 users.

MAC Address Table Attack Mitigation

What makes tools such as **macof** so dangerous is that an attacker can create a MAC table overflow attack very quickly. For instance, a Catalyst 6500 switch can store 132,000 MAC addresses in its MAC address table. A tool such as **macof** can flood a switch with up to 8,000 bogus frames per second; creating a MAC address table overflow attack in a matter of a few seconds.

Another reason why these attack tools are dangerous is because they not only affect the local switch, they can also affect other connected Layer 2 switches. When the MAC address table of a switch is full, it starts flooding out all ports including those connected to other Layer 2 switches.

To mitigate MAC address table overflow attacks, network administrators must implement port security. Port security will only allow a specified number of source MAC addresses to be learned on the port. Port security is further discussed in another module.

10.5 LAN Attacks

Video – VLAN and DHCP Attacks

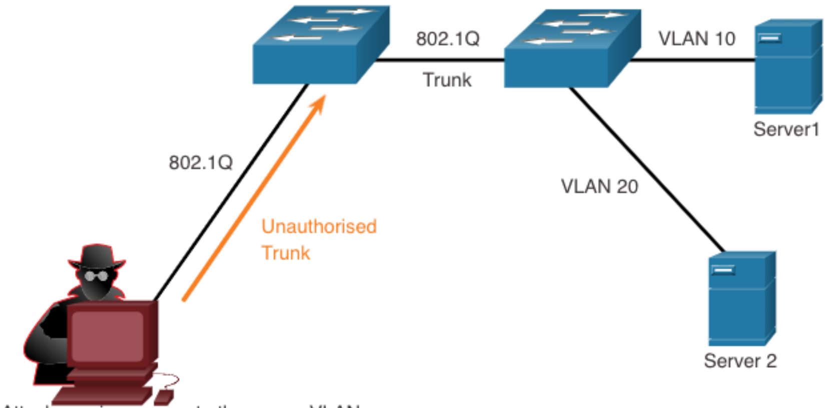
This video will cover the following:

- VLAN Hopping Attack
- VLAN Double-Tagging Attack
- DHCP Starvation Attack
- DHCP Spoofing Attack

VLAN Hopping Attacks

A VLAN hopping attack enables traffic from one VLAN to be seen by another VLAN without the aid of a router. In a basic VLAN hopping attack, the threat actor configures a host to act like a switch to take advantage of the automatic trunking port feature enabled by default on most switch ports.

The threat actor configures the host to spoof 802.1Q signaling and Cisco-proprietary Dynamic Trunking Protocol (DTP) signaling to trunk with the connecting switch. If successful, the switch establishes a trunk link with the host, as shown in the figure. Now the threat actor can access all the VLANs on the switch. The threat actor can send and receive traffic on any VLAN, effectively hopping between VLANs.



Attacker gains access to the server VLAN

VLAN Double-Tagging Attacks

A threat actor is specific situations could embed a hidden 802.1Q tag inside the frame that already has an 802.1Q tag. This tag allows the frame to go to a VLAN that the original 802.1Q tag did not specify.

- **Step 1:** The threat actor sends a double-tagged 802.1Q frame to the switch. The outer header has the VLAN tag of the threat actor, which is the same as the native VLAN of the trunk port.
- **Step 2**: The frame arrives on the first switch, which looks at the first 4-byte 802.1Q tag. The switch sees that the frame is destined for the native VLAN. The switch forwards the packet out all native VLAN ports after stripping the VLAN tag. The frame is not retagged because it is part of the native VLAN. At this point, the inner VLAN tag is still intact and has not been inspected by the first switch.
- **Step 3**: The frame arrives at the second switch which has no knowledge that it was supposed to be for the native VLAN. Native VLAN traffic is not tagged by the sending switch as specified in the 802.1Q specification. The second switch looks only at the inner 802.1Q tag that the threat actor inserted and sees that the frame is destined the target VLAN. The second switch sends the frame on to the target or floods it, depending on whether there is an existing MAC address table entry for the target.

VLAN Double-Tagging Attacks (Cont.)

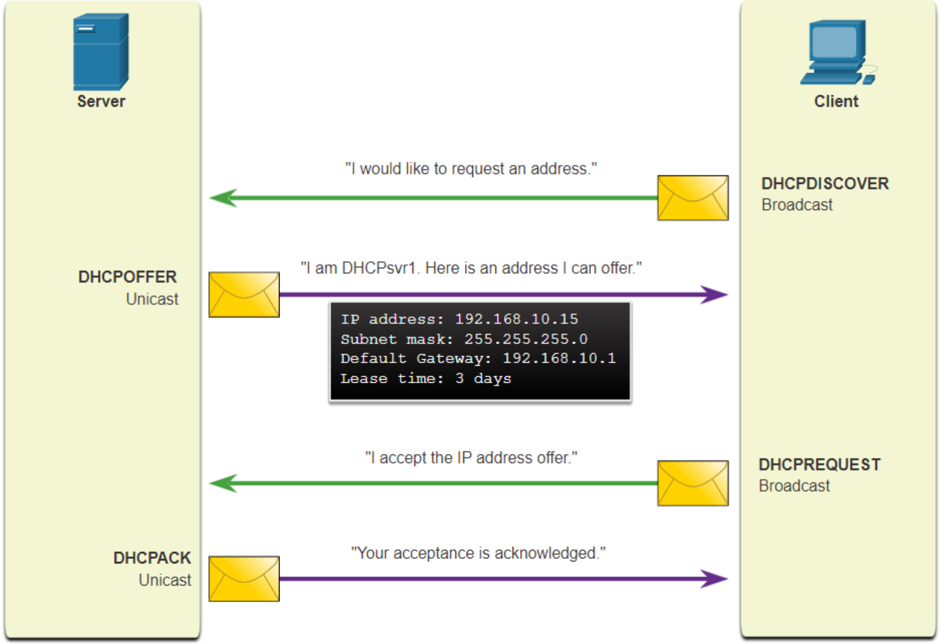
A VLAN double-tagging attack is unidirectional and works only when the attacker is connected to a port residing in the same VLAN as the native VLAN of the trunk port. The idea is that double tagging allows the attacker to send data to hosts or servers on a VLAN that otherwise would be blocked by some type of access control configuration. Presumably the return traffic will also be permitted, thus giving the attacker the ability to communicate with devices on the normally blocked VLAN.

VLAN Attack Mitigation - VLAN hopping and VLAN double-tagging attacks can be prevented by implementing the following trunk security guidelines, as discussed in a previous module:

- Disable trunking on all access ports.
- Disable auto trunking on trunk links so that trunks must be manually enabled.
- Be sure that the native VLAN is only used for trunk links.

DHCP Messages

DHCP servers dynamically provide IP configuration information including IP address, subnet mask, default gateway, DNS servers, and more to clients. A review of the sequence of the DHCP message exchange between client and server is show in the figure.



"I would like to request an address."

"I am DHCPsvr1. Here is an address I can offer."

```
IP address: 192.168.10.15
Subnet mask: 255.255.255.0
Default Gateway: 192.168.10.1
Lease time: 3 days
```

"I accept the IP address offer."

"Your acceptance is acknowledged."

DHCP Attacks

Two types of DHCP attacks are DHCP starvation and DHCP spoofing. Both attacks are mitigated by implementing DHCP snooping.

- **DHCP Starvation Attack** – The goal of this attack is to create a DoS for connecting clients. DHCP starvation attacks require an attack tool such as Gobbler. Gobbler has the ability to look at the entire scope of leasable IP addresses and tries to lease them all. Specifically, it creates DHCP discovery messages with bogus MAC addresses.
- **DHCP Spoofing Attack –** This occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. A rogue server can provide a variety of misleading information, including the following:
  - **Wrong default gateway** - The rogue server provides an invalid gateway or the IP address of its host to create a man-in-the-middle attack. This may go entirely undetected as the intruder intercepts the data flow through the network.
  - **Wrong DNS server** - The rogue server provides an incorrect DNS server address pointing the user to a nefarious website.
  - **Wrong IP address** - The rogue server provides an invalid IP address effectively creating a DoS attack on the DHCP client.

Video – ARP Attacks, STP Attacks, and CDP Reconnaissance

This video will cover the following:

- ARP Spoofing Attack
- ARP Poisoning Attack
- STP Attack
- CDP Reconnaissance

ARP Attacks

- Hosts broadcast ARP Requests to determine the MAC address of a host with a destination IP address. All hosts on the subnet receive and process the ARP Request. The host with the matching IP address in the ARP Request sends an ARP Reply.
- A client can send an unsolicited ARP Reply called a "gratuitous ARP". Other hosts on the subnet store the MAC address and IP address contained in the gratuitous ARP in their ARP tables.
- An attacker can send a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch would update its MAC table accordingly. In a typical attack, a threat actor sends unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway, effectively setting up a man-in-the-middle attack.
- There are many tools available on the internet to create ARP man-in-the-middle attacks.
- IPv6 uses ICMPv6 Neighbor Discovery Protocol for Layer 2 address resolution. IPv6 includes strategies to mitigate Neighbor Advertisement spoofing, similar to the way IPv6 prevents a spoofed ARP Reply.
- ARP spoofing and ARP poisoning are mitigated by implementing Dynamic ARP Inspection (DAI).

Address Spoofing Attacks

- IP address spoofing is when a threat actor hijacks a valid IP address of another device on the subnet or uses a random IP address. IP address spoofing is difficult to mitigate, especially when it is used inside a subnet in which the IP belongs.
- MAC address spoofing attacks occur when the threat actors alter the MAC address of their host to match another known MAC address of a target host. The switch overwrites the current MAC table entry and assigns the MAC address to the new port. It then inadvertently forwards frames destined for the target host to the attacking host.
- When the target host sends traffic, the switch will correct the error, realigning the MAC address to the original port. To stop the switch from returning the port assignment to its correct state, the threat actor can create a program or script that will constantly send frames to the switch so that the switch maintains the incorrect or spoofed information.
- There is no security mechanism at Layer 2 that allows a switch to verify the source of MAC addresses, which is what makes it so vulnerable to spoofing.
- IP and MAC address spoofing can be mitigated by implementing IP Source Guard (IPSG).

STP Attack

- Network attackers can manipulate the Spanning Tree Protocol (STP) to conduct an attack by spoofing the root bridge and changing the topology of a network. Attackers can then capture all traffic for the immediate switched domain.
- To conduct an STP manipulation attack, the attacking host broadcasts STP bridge protocol data units (BPDUs) containing configuration and topology changes that will force spanning-tree recalculations. The BPDUs sent by the attacking host announce a lower bridge priority in an attempt to be elected as the root bridge.
- This STP attack is mitigated by implementing BPDU Guard on all access ports. BPDU Guard is discussed in more detail later in the course.

CDP Reconnaissance

The Cisco Discovery Protocol (CDP) is a proprietary Layer 2 link discovery protocol. It is enabled on all Cisco devices by default. Network administrators also use CDP to help configure and troubleshoot network devices. CDP information is sent out CDP-enabled ports in periodic, unencrypted, unauthenticated broadcasts. CDP information includes the IP address of the device, IOS software version, platform, capabilities, and the native VLAN. The device receiving the CDP message updates its CDP database.

To mitigate the exploitation of CDP, limit the use of CDP on devices or ports. For example, disable CDP on edge ports that connect to untrusted devices.

- To disable CDP globally on a device, use the **no cdp run** global configuration mode command. To enable CDP globally, use the **cdp run** global configuration command.
- To disable CDP on a port, use the **no cdp enable** interface configuration command. To enable CDP on a port, use the **cdp enable** interface configuration command.

Note: Link Layer Discovery Protocol (LLDP) is also vulnerable to reconnaissance attacks. Configure **no lldp run** to disable LLDP globally. To disable LLDP on the interface, configure **no lldp transmit** and **no lldp receive**.

10.6 Module Practice and Quiz

- Cynet XDR provides multiple, integrated prevention
- technologies to block standard and advanced attacks across
- your environment. The detection power achieved by natively
- combining signals and data from multiple sources simply
- cannot be matched by siloed, point protection solutions.

Module Practice and Quiz

What Did I Learn In This Module?

- Endpoints are particularly susceptible to malware-related attacks that originate through email or web browsing, such as DDOS, date breaches, and malware. These endpoints have typically used traditional host-based security features, such as antivirus/antimalware, host-based firewalls, and host-based intrusion prevention systems (HIPSs). Endpoints are best protected by a combination of NAC, host-based AMP software, an email security appliance (ESA), and a web security appliance (WSA).
- AAA controls who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting).
- The IEEE 802.1X standard is a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports.
- If Layer 2 is compromised, then all layers above it are also affected. The first step in mitigating attacks on the Layer 2 infrastructure is to understand the underlying operation of Layer 2 and the Layer 2 solutions: Port Security, DHCP Snooping, DAI, and IPSG. These won’t work unless management protocols are secured.

What Did I Learn In This Module? (Cont.)

- MAC address flooding attacks bombard the switch with fake source MAC addresses until the switch MAC address table is full.
- A VLAN hopping attack enables traffic from one VLAN to be seen by another VLAN without the aid of a router.
- A VLAN double-tagging attack is unidirectional and works only when the threat actor is connected to a port residing in the same VLAN as the native VLAN of the trunk port.
- VLAN hopping and VLAN double-tagging attacks can be prevented by implementing the following trunk security guidelines:
  - Disable trunking on all access ports.
  - Disable auto trunking on trunk links so that trunks must be manually enabled.
  - Be sure that the native VLAN is only used for trunk links.
- Two types of DHCP attacks are DHCP starvation and DHCP spoofing. Both attacks are mitigated by implementing DHCP snooping.

What Did I Learn In This Module? (Cont.)

- ARP Attack: A threat actor sends a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch updates its MAC table accordingly. Now the threat actor sends unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway. ARP spoofing and ARP poisoning are mitigated by implementing DAI.
- Address Spoofing Attack: IP address spoofing is when a threat actor hijacks a valid IP address of another device on the subnet or uses a random IP address. MAC address spoofing attacks occur when the threat actors alter the MAC address of their host to match another known MAC address of a target host. IP and MAC address spoofing can be mitigated by implementing IPSG.
- STP Attack: Threat actors manipulate STP to conduct an attack by spoofing the root bridge and changing the topology of a network. Threat actors make their hosts appear as root bridges; therefore, capturing all traffic for the immediate switched domain. This STP attack is mitigated by implementing BPDU Guard on all access ports.
- CDP Reconnaissance: CDP information is sent out CDP-enabled ports in periodic, unencrypted broadcasts. CDP information includes the IP address of the device, IOS software version, platform, capabilities, and the native VLAN. The device receiving the CDP message updates its CDP database. the information provided by CDP can also be used by a threat actor to discover network infrastructure vulnerabilities. To mitigate the exploitation of CDP, limit the use of CDP on devices or ports.

cisco